RICARDO AUGUSTO MIGUEL

ANÁLISE DE RISCOS DE SEGURANÇA EM APLICAÇÕES ERP BASEADAS EM AMBIENTES DE COMPUTAÇÃO EM NUVEM

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para conclusão do curso de MBA em Tecnologia de Software.

São Paulo

2014

RICARDO AUGUSTO MIGUEL

ANÁLISE DE RISCOS DE SEGURANÇA EM APLICAÇÕES ERP BASEADAS EM AMBIENTES DE COMPUTAÇÃO EM NUVEM

Monografia apresentada ao PECE – Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo como parte dos requisitos para a conclusão do curso de MBA em Tecnologia de Software.

Área de Concentração: Tecnologia de Software

Orientador: Prof. Dr. Marcos A. Simplicio Jr.

São Paulo

2014

DEDICATÓRIA

Dedico este trabalho em especial a meus pais que me deram todo o suporte na minha formação.

Aos meus irmãos.

A minha esposa Carolina, pela paciência e incentivo.

AGRADECIMENTOS

À Escola Politécnica da Universidade de São Paulo – EPUSP e ao PECE – Programa de Educação Continuada em Engenharia por possibilitar a realização e o desenvolvimento da pesquisa elaborada neste trabalho.

Aos meus colegas de curso pelo apoio, amizade e considerações.

Em especial à minha família.

RESUMO

O objetivo deste trabalho é analisar e discutir sobre a segurança e privacidade de dados de aplicações ERP na nuvem. Assim, são levantados os benefícios (em termos financeiros e de flexibilidade) e riscos para este tipo de cenário comparando-os com os ambientes tradicionais.

Primeiramente são apresentados os conceitos de computação em nuvem, suas características, modelos de implantação e modelos de serviço.

A seguir são apresentados e discutidos os benefícios e riscos da computação em nuvem, destacando os pontos fortes e fracos deste tipo de cenário em aplicações críticas, com foco especial em características que podem afetar ERPs.

Por fim, são apresentados estudos nos quais se discute a visão de diversas empresas com relação ao modelo de ERP baseado na nuvem em contraste com ERPs tradicionais. Essa discussão é concluída com uma análise comparativa entre duas aplicações ERP produzidas e comercializadas pela SAP usando ambos os modelos, buscando elucidar as diferenças das aplicações para cada tipo de ambiente.

ABSTRACT

The goal of this work is to analyze and discuss data security and privacy in cloud-based ERP applications. Specifically, we evaluate the benefits (in terms of financial and flexibility) and risks for this type of scenario, comparing them with traditional environments.

First, we present the concept of cloud computing and its characteristics, as well as its implementation and service models.

Then, we present and discuss the benefits and risks of cloud computing, highlighting the strengths and weaknesses of this type of scenario in critical applications, focusing specifically on issues that may affect ERPs.

Finally, we present studies that discuss how companies see the cloud-based ERP model in contrast with traditional ERPs. This discussion is concluded with a comparative analysis between two ERP applications produced and commercialized by SAP, trying to elucidate the differences between the applications for each type of environment.

LISTA DE ILUSTRAÇÕES

Pág.

Figura 2.1 - Variação dos modelos Público, Privado e Híbrido..... 21
Figura 2.2 - Representação de um serviço SaaS. 22
Figura 2.3 - Correio eletrônico oferecido por um provedor de serviços. 23
Figura 2.4 - Plataforma como serviço. 24
Figura 2.5 - Representação do serviço IaaS..... 25
Figura 2.6 - Principais preocupações na adoção de um ERP na nuvem..... 27
Figura 2.7 - Segurança X Tamanho da organização 29
Figura 2.8 - Segurança X Investimento em ERP 30
Figura 3.1 - Resultados da pesquisa IDC sobre as preocupações de segurança 32
Figura 3.2 - Distribuição dos Riscos..... 36
Figura 3.3- Interface web de administração do ERP na nuvem..... 43
Figura 4.1 - Aplicação SAP® Business One 50
Figura 4.2 - Arquitetura SAP® Business One OnDemand..... 51
Figura 4.3 - SAP® Business One OnDemand - Portal de acesso web..... 52

LISTA DE TABELAS

Pág.

Tabela 2.1 - Modelo de implantação da nuvem, conforme definições do NIST 20
Tabela 2.2 - Comparação entre ERP tradicional e ERP na nuvem 28
Tabela 2.3 - Riscos entre ERP Tradicional e ERP na nuvem 28
Tabela 4.1 - Custos de implementação das aplicações SAP 53

LISTA DE ABREVIATURAS E SIGLAS

API - *Application Programming Interface* (Interface de Programação de Aplicativos)

BI - *Business Intelligence*

COM - *Component Object Model*

CRM - *Customer Relationship Management*

ERP – *Enterprise Resource Planning* (Sistema Integrado de Gestão Empresarial)

IP - *Internet Protocol*

MRP - *Manufacturing Resource Planning*

PME – Pequenas e Médias Empresas

SLA - *Service Level Agreement* (Acordo de Nível de Serviço)

SPAM - *Sending and Posting Advertisement in Mass*

SSL - *Secure Sockets Layer*

TCO - *Total cost of ownership*

TI – Tecnologia da Informação

XML - *eXtensible Markup Language*

SUMÁRIO

Pág.

1 Introdução 13

1.1 Objetivos do trabalho 13

1.2 Motivação e Justificativa 14

1.3 Organização do Trabalho 15

2 Computação em nuvem 16

2.1 Características essenciais 17

2.2 Modelos de implantação 18

2.3 Modelos de serviço 21

2.3.1 Software como um Serviço (SaaS – *Software as a Service*) 21

2.3.2 Plataforma como um Serviço (PaaS – *Platform as a Service*) 23

2.3.3 Infraestrutura como um Serviço (IaaS – *Infrastructure as a Service*) 24

2.4 ERP na nuvem 25

2.4.1 Definição de ERP 25

2.4.2 Análise do ERP na nuvem 26

3 Segurança na Computação em nuvem 31

3.1 Benefícios 32

3.1.1 Dados logicamente centralizados 33

3.1.2 Redução na perda/roubo dos dados 33

3.1.3 Monitoramento 34

3.1.4 Troca imediata em caso de falha 34

3.1.5 Registro das transações 34

3.1.6 Compilações seguras 34

3.1.7 Melhoria de segurança do software 35

3.1.8 Testes de segurança 35

3.2 Riscos 35

3.2.1 Riscos políticos e organizacionais 37

3.2.2 Riscos Técnicos 41

3.2.3 Riscos Legais 47

4 Estudo de caso: Aplicação ERP na nuvem 49

4.1 Aplicação SAP tradicional *vs.* nuvem 49

4.1.1 SAP® Business One (*local*) 49

4.1.2 SAP® Business One OnDemand 50
4.1.3 Análise 52
5 Considerações Finais 55
5.1 Contribuições do Trabalho 55
5.2 Trabalhos Futuros 56
6 Referências 57
7 APÊNDICE I – Tabelas de análise de riscos da computação em nuvem 59

1 Introdução

Com o crescente e acelerado avanço tecnológico e a disponibilidade de Internet com velocidade cada vez maior, grande parte das empresas vem buscando a utilização de recursos oferecidos pela computação em nuvem (*cloud computing*). A grande motivação na utilização deste tipo de tecnologia é a possibilidade de se ter uma poderosa infraestrutura de servidores e serviços por um custo mais acessível do que o obtido utilizando modelos tradicionais. Portanto, a nuvem pode ser considerada um modelo eficiente para o armazenamento e processamento de dados entre diferentes tipos de dispositivos e tecnologias através da Internet. Além disso, ela traz facilidades diversas, pois não é preciso a instalação de aplicativos, ou a aquisição e manutenção de servidores e banco de dados dentro da empresa. Entretanto, é necessário atentar-se para a segurança da informação neste contexto. Afinal, informações importantes como dados de clientes, faturamento, recursos humanos, entre outros, não estão mais sob o domínio da própria empresa, e sim do provedor de serviço de computação em nuvem.

1.1 Objetivos do trabalho

Este trabalho tem como objetivo discutir as principais preocupações que pequenas e médias empresas (PME) devem ter na migração dos seus dados para a nuvem. Além de um estudo teórico, também é apresentado um estudo de caso de uma aplicação de gestão empresarial integrada (*Enterprise Resource Planning* - ERP) denominada SAP® Business One OnDemand[1], produzida e comercializada pela SAP AG. O interesse nessa aplicação específica é que a mesma é uma versão

[1] http://www.sap.com/solution/sme/software/erp/small-business-management/cloud/index.html

para nuvem do SAP® Business One[2], uma aplicação amplamente utilizada porém instalada localmente no cliente.

1.2 Motivação e Justificativa

Reduzir custos na área de TI sempre foi um objetivo primário em diversas empresas. Isso ocorre porque a área de TI, assim como qualquer outra área de apoio (Recursos humanos, Qualidade, Controle de patrimônio, etc.) não está ligada diretamente à geração de receitas de diversas companhias. Assim, com a chegada da computação em nuvem, muitas empresas têm visto nesta tecnologia mais uma forma de redução de custos, tanto de mão de obra (analistas) como de infraestrutura (hardware, software, etc.). Outro fator importante que é muitas vezes apresentado como um fator atrativo da computação em nuvem é a preocupação ambiental. A computação em nuvem está ligada diretamente com a virtualização de servidores, que é uma técnica empregada pelos *datacenters* para consolidação, em apenas um hardware, de dois ou mais servidores virtuais. E como consequência desta virtualização acontece uma redução no consumo de energia, o que remete ao conceito de "TI verde" [VERAS, 2011].

Esta crescente atração pela computação em nuvem é relativamente recente, de modo que as questões de segurança envolvidas na sua adoção ainda não são bem compreendidas. Assim, o estudo da literatura sobre segurança em nuvem e sua aplicação em um cenário real ganham interesse para a melhor compreensão dos riscos envolvidos nessa tecnologia. Afinal, o que se imagina ser uma solução pode tornar-se um pesadelo para as organizações se algumas medidas prévias não forem tomadas. Desta forma, a contribuição desta monografia é alertar para algumas das principais precauções que as empresas devem tomar antes de migrar seus dados para um ambiente em nuvem.

[2] http://www.sap.com/brazil/solution/sme/software/erp/small-business-management/overview/index.html

1.3 Organização do Trabalho

O restante do presente trabalho está organizado da seguinte forma

O Capítulo 2 apresenta os conceitos, paradigmas e as características da computação em nuvem, discutindo também os diferentes tipos de serviços oferecidos.

O Capítulo 3 apresenta os fundamentos de segurança da informação específicos para este tipo de ambiente.

O Capítulo 4 descreve o estudo de uma aplicação comercial de ERP baseada em nuvem, cenário em que são avaliados os riscos relativos às informações tratadas e como elas estão expostas a terceiros.

O Capítulo 5 apresentada as considerações finais do trabalho, incluindo uma discussão sobre as tendências desta tecnologia e sugestões para trabalhos futuros nesta área.

O APÊNDICE I apresenta as tabelas de análise de riscos da computação em nuvem.

2 Computação em nuvem

Computação em nuvem é um novo método para prover computação em forma de serviço através da Internet. Dentre os diversos serviços que podem ser implementados usando esse modelo, podem ser citadas aplicações de e-mail, calendários, planilhas de textos, etc., como aqueles fornecidos pelo Google[3] e Apple[4], por exemplo. Outra forma de serviço oferecido são servidores, banco de dados, etc., como os que são fornecidos pela Amazon[5], Google[6] e Microsoft[7], por exemplo.

Um dos pontos fortes da computação em nuvem e que vem despertando grande interesse nas empresas é a promessa de alta qualidade de infraestrutura e serviços por um baixo custo [KIADEHI e MOHAMMADI, 2012] e sem a necessidade de uma grande atuação da equipe interna de TI, deixando com que a mesma se concentre mais com planos estratégicos ao invés de se preocupar em manter o *datacenter* em funcionamento [VELTE, VELTE e ELSENPETER, 2010]. Outro ponto importante a ser considerado diz respeito à escalabilidade e flexibilidade de recursos. Um exemplo prático é um site de venda de ingressos online. Quando não existe qualquer evento de grande público, tal site não precisa de muitos recursos de hardware, como processamento e memória, mas apenas o suficiente para se manter acessível a todos. Suponha então que, por um determinado período, esse mesmo site passe a vender os ingressos para um evento de massa, como a Copa do Mundo FIFA. Nesse período, ele necessitará de maior poder de processamento e largura de banda para atender à demanda. Com o uso da nuvem, em poucos segundos e de forma automática os seus servidores vão se multiplicando e aumentado o seu poder de processamento para atender todas as requisições sem comprometer o desempenho, de forma transparente ao cliente. Juntamente com essa elasticidade no uso de recursos, na nuvem é possível também a utilização do modelo de

---

[3] https://docs.google.com/

[4] http://www.icloud.com/

[5] http://aws.amazon.com/pt/ec2/

[6] http://appengine.google.com/

[7] http://azure.microsoft.com/pt-br/

pagamento conhecido como "pay-as-you-go", ou seja, o cliente paga apenas pela quantidade de serviço utilizado (e.g., tarifado por hora).

2.1 Características essenciais

Segundo o Instituto Nacional de Padrões e Tecnologias dos Estados Unidos (*National Institute of Standards and Technology* -- NIST) [MELL e GRANCE, 2011], a computação em nuvem como um modelo de computação é definida por cinco características essenciais:

- Auto-serviço sob demanda: Os recursos computacionais, como processamento e/ou espaço em disco, podem ser providos automaticamente, sem a necessidade de interação humana. Geralmente, a administração dos limites desejados do serviço é feita pelo próprio usuário, através de uma interface web.

- Acesso amplo à rede: Os recursos computacionais estão disponíveis através da Internet e podem ser acessados por diferentes plataformas através de mecanismos e protocolos padrão.

- Agrupamento de recursos: Os recursos computacionais do provedor (armazenamento, processamento, memória) são alocados e realocados de forma dinâmica de acordo com a demanda, para servir a múltiplos usuários. Geralmente, o cliente não tem controle ou conhecimento da localização física exata dos recursos. No serviço Amazon EC2, por exemplo, o cliente pode escolher a região em que ficarão alocados os recursos (Tóquio, Cingapura, Sydney, São Paulo, entre outros), mas não sabe sua localização exata [AMAZON].

- Elasticidade Rápida: Os recursos devem ser providos de forma rápida e elástica de acordo com a demanda do cliente, dando a impressão de que ele

possui recursos ilimitados. Vale lembrar que esta elasticidade pode ser tanto para cima, como para baixo, ou seja, o cliente pode aumentar ou diminuir os recursos de forma rápida e de acordo com a sua necessidade.

- Serviço Mensurado: O uso para cada tipo de serviço (processamento, armazenamento e largura de banda) deve ser monitorado, controlado e reportado para ambas as partes (provedor e consumidor). Sendo assim, o cliente tem a possibilidade de pagar apenas pela quantidade de recurso utilizado.

2.2 Modelos de implantação

Segundo o NIST [MELL e GRANCE, 2011], são oferecidos quatro modelos básicos para a implantação da computação em nuvem: nuvem privada, pública, comunitária ou híbrida (veja Tabela 2.1). A escolha do modelo a ser utilizado depende da necessidade da empresa e de suas particularidades. As características de cada modelo são discutidas abaixo:

- **Nuvem Privada (Private Cloud)** – Neste modelo a infraestrutura de nuvem é disponibilizada para o cliente de forma privada, ou seja, o acesso à nuvem é feito exclusivamente pelo cliente que contratou o serviço. A infraestrutura poderá estar no próprio cliente ou ser fornecida por um terceiro. Em comparação com os outros modelos de implantação de nuvem, este pode ser considerado o mais seguro e que proporciona o melhor desempenho, justamente por não ser compartilhado com outros clientes. Mas também é o modelo que gera mais custos para a empresa, já que por ter o seu controle feito internamente pela equipe de TI necessita de profissionais mais capacitados e especialistas no assunto. Se o cliente optar por manter a infraestrutura internamente, efetuando a aquisição de servidores, por exemplo, a economia diminui ainda mais. [CASTRO e SOUSA]

- **Nuvem Pública (Public Cloud)** – Neste modelo a infraestrutura de nuvem é fornecida por um terceiro, geralmente um provedor de nuvem (Cloud Provider) e é compartilhada por múltiplos clientes. Este tipo de modelo é o mais interessante quando o quesito é economia, por ser um recurso compartilhado. Neste tipo de infraestrutura, é comum o uso de máquinas virtuais, onde o provedor de serviços, através de software específicos de *Hypervisor* compartilham o hardware (Processador, memória, rede, etc) e os clientes acessam os serviços através de um navegador web. Neste tipo de modelo é comum os clientes pagarem apenas pelo recurso utilizado, técnica conhecida como "Pay-as-you-go". Por exemplo, o serviço EC2, fornecido pela Amazon, cobra alguns centavos pelo uso de máquinas virtuais [KIADEHI e MOHAMMADI, 2012].

- **Nuvem Comunitária (Community Cloud)** – Este formato representa um cenário mais complexo e com uma infinidade de possíveis papéis e interações. Geralmente é feito pelo compartilhamento de uma nuvem por diversas empresas com interesses semelhantes. Diferente dos modelos acima, neste modelo os dados de um cliente podem ser armazenados com os dados de outros clientes, desde que pertençam a mesma comunidade [CASTRO e SOUSA].

- **Nuvem Híbrida (Hybrid Cloud)** – A exemplo do modelo anterior, este também representa um cenário mais complexo, pelo falo de ser combinado dois ou mais modelos de implantação (privada, pública ou comunitária). A utilização deste modelo requer um trabalho minucioso de rotulagem de dados, para garantir que os dados de nuvem privada não sejam disponibilizados na nuvem pública [CASTRO e SOUSA]. Um exemplo da utilização deste modelo pode ser encontrado em uma empresa que possui sua infraestrutura de forma privada, mas para fins de redundância (tolerância contra falhas) possui uma infraestrutura em nuvem pública como mecanismo de contingência [MAUSER e DIOGENES, 2013].

Tabela 2.1 - Modelo de implantação da nuvem, conforme definições do NIST

Adaptado de [MELL e GRANCE, 2011]

Modelo	Definição	Aplicação
Privada	Infraestrutura controlada por uma organização e disponibilizada apenas para seus usuários.	Otimização dos recursos internos, integração de sistemas e ativos de uma mesma empresa.
Pública	Infraestrutura controlada por uma organização e disponibilizados para a outra organizações e usuários em geral.	SaaS e outros serviços de utilidade pública, incluindo e-mail, ferramentas de escritório e outras aplicações.
Comunitária	Infraestrutura controlada e usada por um grupo de instituições com objetivos e necessidades em comum.	Universidades e experimentos científicos.
Híbrida	Infra-estrutura composta por várias nuvens (possivelmente a partir de diferentes modelos de implantação).	Integração de nuvens e sistemas distribuídos, agregação de infra-estrutura.

De um modo geral, a oferta de serviços, o custo, a responsabilidade e a garantia (e.g., de segurança) dos modelos de implantação da nuvem variam de acordo com a necessidade do cliente. A Figura 2.1 ajuda a compreender esta variação. Em um modelo Público, a oferta de serviços é maior se comparada ao modelo Privado; em compensação, o custo, a responsabilidade e as garantias são menores.

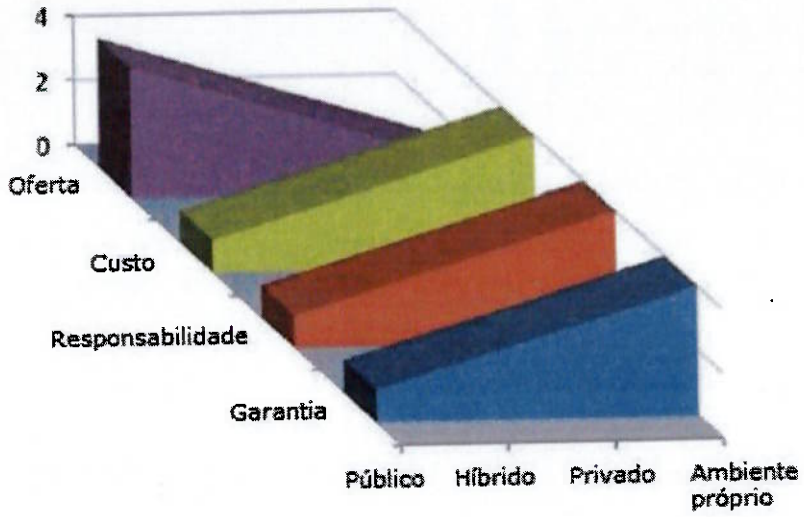

Figura 2.1 - Variação dos modelos Público, Privado e Híbrido.
Adaptado de [ENISA]

2.3 Modelos de serviço

Segundo o NIST [MELL e GRANCE, 2011], existem três diferentes formas básicas para o consumo de diferentes serviços de computação em nuvem conhecidas pelas siglas SaaS, Paas e IaaS. Cada uma delas é discutida a seguir:

2.3.1 Software como um Serviço (SaaS – *Software as a Service*)

Nesse modelo, o software é executado em um servidor, ou seja, não é necessária a instalação da aplicação na estação de trabalho do cliente. O acesso é feito através de um navegador web, ou por meio de qualquer dispositivo conectado na Internet. A Figura 2.2 representa esse modelo de serviço.

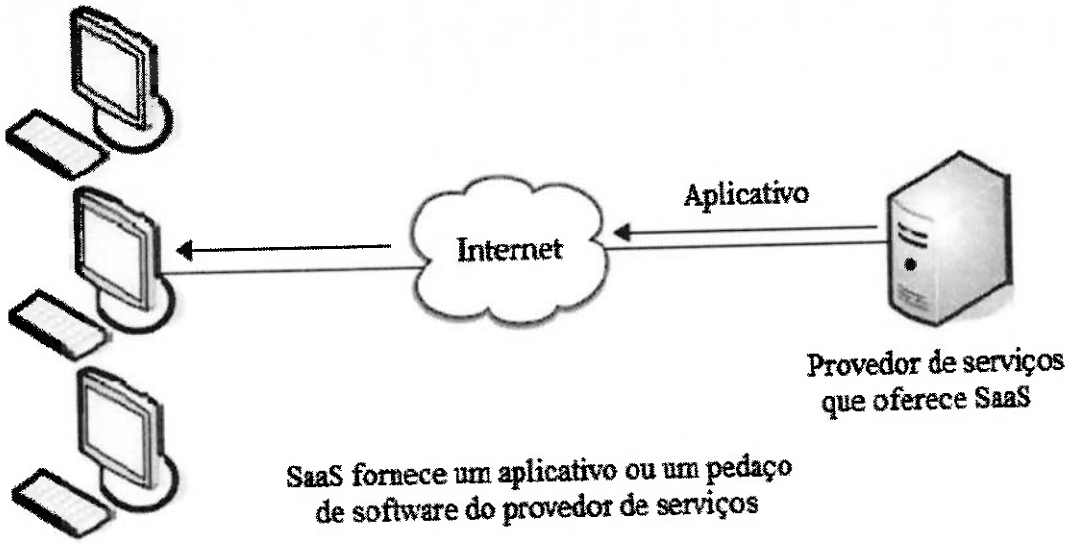

Figura 2.2 - Representação de um serviço SaaS.
Extraído de [VELTE, VELTE e ELSENPETER, 2010]

Esse é provavelmente o modelo de serviço que traz maiores reduções de custos para a empresa, já que o cliente não precisa adquirir o software e as licenças de uso, nem estações de trabalho com grande desempenho. Além disso, ele traz facilidades pelo fato de não necessitar de instalações e atualizações. Seguindo o modelo de pagamento sob demanda, o cliente paga apenas pelo tempo e, em alguns casos, apenas pelos recursos que utilizar.

É interessante notar que, apesar de a computação em nuvem ser algo relativamente novo, esse modelo de serviço já existe há um bom tempo. Um exemplo simples são os serviços de correio eletrônico fornecidos aos usuários, como o Hotmail [18], Gmail [17], Yahoo [19] entre outros, conforme ilustrado na Figura 2.3.

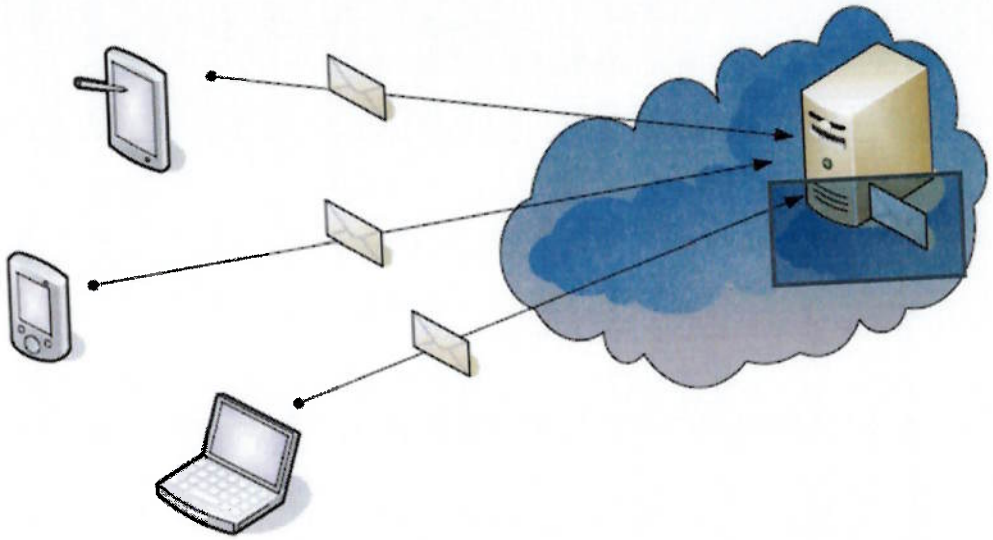

Figura 2.3 - Correio eletrônico oferecido por um provedor de serviços.
Extraído de [MAUSER e DIOGENES, 2013]

2.3.2 Plataforma como um Serviço (PaaS – *Platform as a Service*)

Nesse modelo, é fornecido ao cliente uma infraestrutura de TI (software e hardware) para desenvolvimento e utilização de aplicações baseadas na web, como servidores para aplicações web e serviço de banco de dados. Desta forma, este modelo difere do SaaS porque, ao invés de abrigar a aplicação pronta, a nuvem fornece todo o suporte necessário para que essa aplicação seja desenvolvida, testada e operada, sendo que o próprio cliente é responsável por desenvolver a aplicação [VELTE, VELTE e ELSENPETER, 2010]. Assim, não é necessário que o cliente configure o ambiente nem se preocupe com a manutenção do hardware ou do software de base que sua aplicação usa (e.g., ambientes de desenvolvimento, compiladores e interpretadores, bancos de dados, sistema operacional, etc.).

Um exemplo de uma oferta desse tipo de plataforma é o provedor de serviços Force.com, que fornece aplicações de software de apoio ao SalesForce.com. APIs e ferramentas de desenvolvimento são fornecidas para dar suporte às aplicações SalesForce [RAINES, 2009]. A Figura 2.4 ilustra este tipo de ambiente.

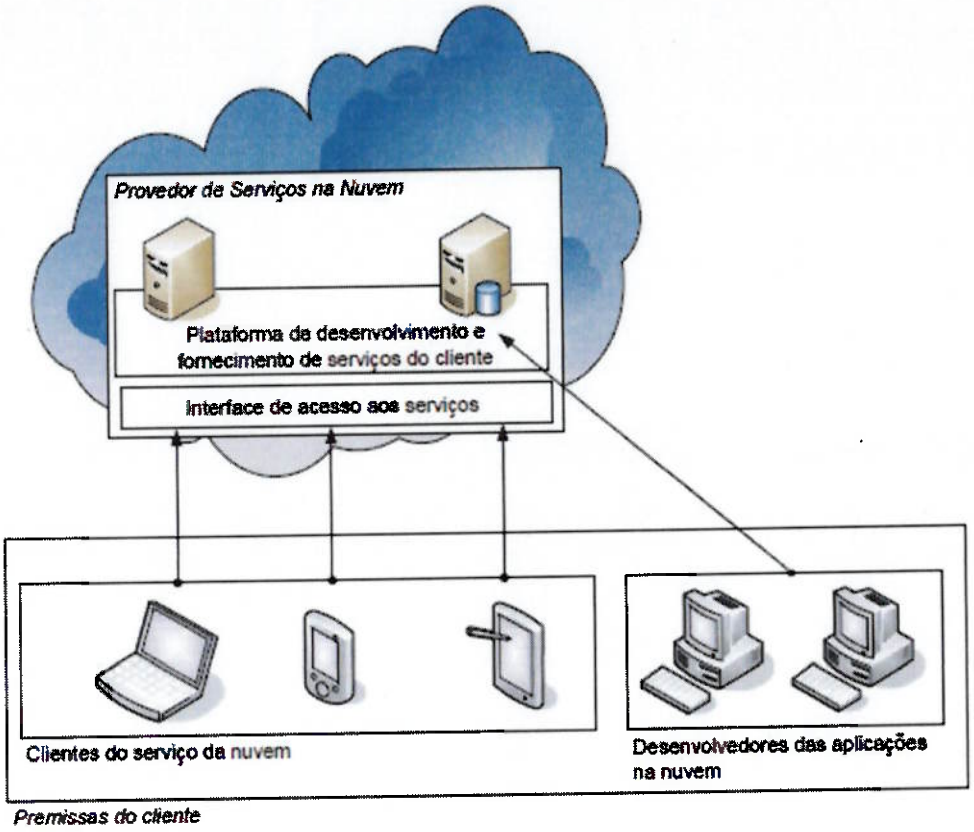

Figura 2.4 - Plataforma como serviço.
Extraído de [MAUSER e DIOGENES, 2013]

2.3.3 Infraestrutura como um Serviço (IaaS – *Infrastructure as a Service*)

Nesse modelo, também conhecido como HaaS (*Hardware as a Service* -- Hardware como um Serviço) [RAINES, 2009], é fornecido pelo provedor de serviços toda a infraestrutura de hardware (geralmente virtualizado) necessária para que o cliente coloque seu negócio em produção. Desta forma, os recursos fornecidos costumam incluir a disponibilização de rede, energia, refrigeração e recursos computacionais (memória, processador, armazenamento) que podem ser acessados através da Internet (veja Figura 2.5). O que difere este dos outros modelos é que o cliente é responsável pelo sistema operacional e também pela manutenção e atualização do software nele executado.

A vantagem desse modelo é que o cliente não precisa manter toda a estrutura física de um *datacenter*, ou seja, o cliente não precisa comprar o hardware e nem

mantê-lo atualizado, tampouco se preocupar com cabeamento, estrutura e segurança física, entre outros [MAUSER e DIOGENES, 2013].

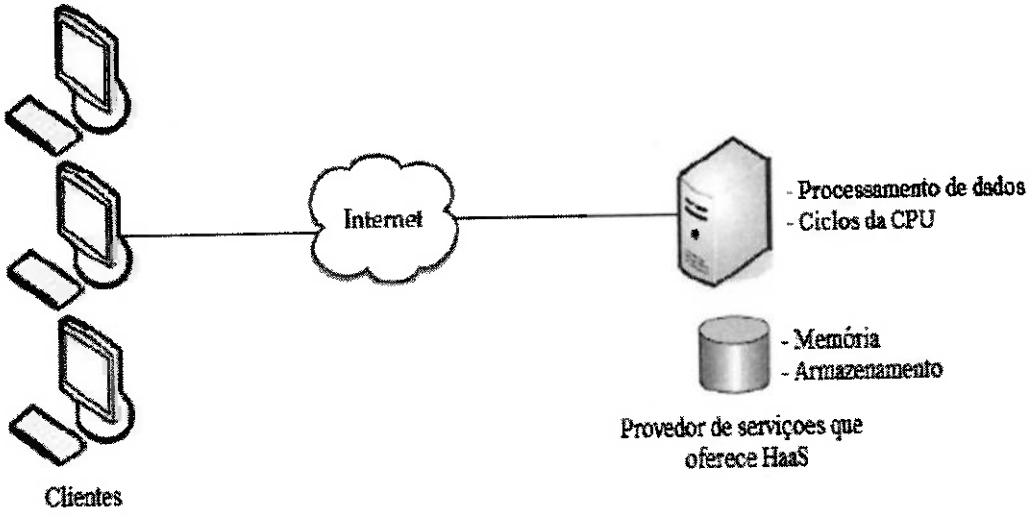

Figura 2.5 - Representação do serviço IaaS.
Extraído de [VELTE, VELTE e ELSENPETER, 2010]

2.4 ERP na nuvem

Os custos de uma implementação de um ERP em ambiente próprio são relativamente altos para pequenas e médias empresas. Esses custos incluem: hardware, software, treinamento, implementação, manutenção, consultoria, entre outros. Portanto, como forma de redução de custos, as organizações de pequeno porte têm recorrido ao uso de ERP na nuvem, ou seja, um ERP hospedado em um provedor de nuvem [KIADEHI e MOHAMMADI, 2012].

2.4.1 Definição de ERP

Apesar de a sigla ERP ter surgido apenas na década de 1990, o conceito já vem sendo usado desde 1960 com a utilização de um sistema para controle de estoque pelas organizações. Como evolução desse sistema, foram adicionadas novas funcionalidades de marketing e planejamento de ordens de produção e compra de materiais, surgindo assim em 1970 a sigla MRP (*Material Resource*

Planning) e posteriormente, em 1980, a sigla MRPII. [KIADEHI e MOHAMMADI, 2012]

O conceito moderno de ERP é um sistema de informação responsável por reunir todas as informações de uma organização, proporcionando a empresa uma visão mais ampla do negócio. Assim, o sistema ERP é responsável por controlar desde a aquisição da matéria-prima até a entrega do produto ao cliente final. [CHOPRA e MEINDL, 2002]

Os sistemas ERPs são formados por diversos módulos, que podem ser personalizados de acordo com os processos de cada organização. Cada módulo atende a uma área de negócio específica e em alguns casos estes módulos são interligados entre si, para atender a outras áreas. Dentre os principais módulos de um ERP, podem ser citados: finanças, logística, fabricação, atendimento do pedido, recursos humanos e gerenciamento de fornecedor.

Pode-se afirmar que sistemas ERPs melhoram os processos de negócios e aumentam o valor da organização. Portanto, o ERP torna-se um elemento importante para a competitivade das empresas. Além disso, os ERPs tendem a melhorar o atendimento ao cliente, baixar níveis de estoque e permitir uma maior atuação global. [LEWANDOWSKI, SALAKO e GARCIA-PEREZ, 2013]

Apesar de o ERP ser uma ferramenta interessante para planejar os recursos de uma empresa, ele fornece apenas uma visão operacional do negócio, ou seja, sua capacidade analítica é relativamente fraca. Mas isso vem mudando com o tempo, pois sistemas de ERP estão em constante evolução. Um exemplo disso são as ferramentas de BI (*Business Intelligence*), que se integram aos sistemas ERPs preexistentes para extrair informações analíticas, ajudando nas tomadas de decisões.

2.4.2 Análise do ERP na nuvem

Basicamente existem dois tipos de implementação de ERPs na nuvem: SaaS e IaaS. O modelo SaaS, como característica própria deste tipo de modelo, possui um baixo custo de aquisição e implementação. Por outro lado, esse tipo de modelo traz limitações e problemas com segurança e privacidade dos dados, pois o provedor tem acesso total aos dados da organização. Já no segundo tipo de implementação,

o ERP pode ser implementado no modelo IaaS fornecido por um provedor ou dentro da própria organização. Com o uso de recursos próprios da organização, aumenta-se consideravelmente a segurança, privacidade e disponibilidade dos dados, embora potencialmente haja menor redução de custos com implementação e manutenção. Já na utilização de infraestrutura fornecida por um provedor, a redução dos custos é maior, mas novamente perde-se em segurança e disponibilidade, conforme discutido anteriormente.

Uma pesquisa realizada com empresas que implementaram o ERP na nuvem utilizando o modelo SaaS deixou evidente que as principais preocupações com relação ao ERP ainda são as mesmas da implementação do ERP tradicional [LEWANDOWSKI, SALAKO e GARCIA-PEREZ, 2013]. Mais especificamente, conforme mostrado na Figura 2.6, as organizações ainda não se preocupam tanto com os riscos típicos da nuvem de ter seus dados expostos a terceiros ou ficarem aprisionados a um fornecedor, se comparados com problemas como personalizações e integração com outros sistemas.

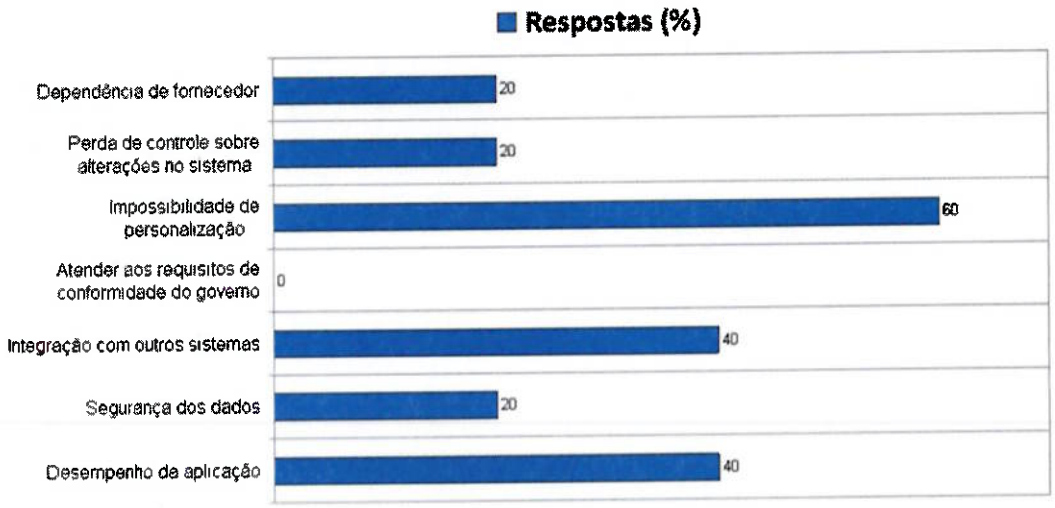

Figura 2.6 - Principais preocupações na adoção de um ERP na nuvem
Adaptado de [LEWANDOWSKI, SALAKO e GARCIA-PEREZ, 2013]

A Tabela 2.2 compara diferentes aspectos de ERPs em ambiente próprio e na nuvem. Embora possam ser levantadas diversas métricas que os diferenciem, a grande diferença está basicamente na disponibilidade dos dados. Isto ocorre porque um ERP na nuvem exige necessariamente uma conexão com a Internet para o seu acesso, o que por um lado permite seu acesso de qualquer lugar e por outro

potencialmente leva aos problemas de segurança que serão detalhados posteriormente no Capítulo 3.

Tabela 2.2 - Comparação entre ERP tradicional e ERP na nuvem
Adaptado de [KIADEHI e MOHAMMADI, 2012]

Fator	ERP local	ERP na nuvem
Redução de custos	Baixa	Alta
Redução na Equipe de TI	Nenhuma	Alta
Custos de implementação	Altos	Baixos
Despesas recorrentes	Relativamente altas	Baixas
Controle sobre o ERP	Facilmente controlável	Difícil de controlar
Custos com suporte	Relativamente altos	Baixos
Custos com licença	Altos	Baixos
Atualização do ERP	Alto custo	Baixo custo
Internet	Não requerido	Requerido

A computação em nuvem, apesar de ser um ambiente teoricamente mais seguro e melhor controlado se comparado com ambiente próprio, possui uma grande quantidade de riscos e problemas com segurança. Por se tratar de um ambiente compartilhado, desperta mais interesses de *hackers*, o que acaba pondo em risco o ERP na nuvem se comparado com o ERP em ambiente próprio. Os riscos e problemas que envolvem a computação em nuvem e sua relação com os ERPs para este cenário serão detalhados posteriormente no Capítulo 3.2.

A Tabela 2.3 apresenta uma análise comparativa dos riscos entre estes dois tipos de cenário.

Tabela 2.3 - Riscos entre ERP Tradicional e ERP na nuvem
Adaptado de [KIADEHI e MOHAMMADI, 2012]

Fator de risco	ERP local	ERP na nuvem
Disponibilidade de Dados (Continuidade do negócio)	Baixa	Alta
Confidencialidade dos dados	Baixa	Alta
Ataques contra ambiente compartilhado	Baixo	Alto
Questões de segurança da Internet	Baixa	Alta

Tabela 2.3 - Riscos entre ERP Tradicional e ERP na nuvem (cont.)

Fator de risco	ERP local	ERP na nuvem
Riscos de espionagem	Baixo	Alto
Privacidade	Baixa	Alta
Usuários com acesso privilegiado	Baixo	Alto
Sanções e localização dos dados	Baixa	Alta
Recuperação de dados	Alta	Baixa
Viabilidade a longo prazo	Alta	Baixa
Riscos desconhecidos	Baixo	Alto

Os riscos apontados na Tabela 2.3 indicam que a utilização do ERP na nuvem leva a um nível de preocupação mais alto se comparado com o ERP em ambiente próprio. Em contrapartida, a mesma Tabela 2.3 apresenta um nível superior de privacidade e disponibilidade dos dados na utilização do ERP na nuvem. Assim, caso a organização possua dados confidenciais e a eventual exposição dos mesmos comprometam a continuidade do negócio, é altamente recomendável a utilização de uma nuvem privada no modelo IaaS.

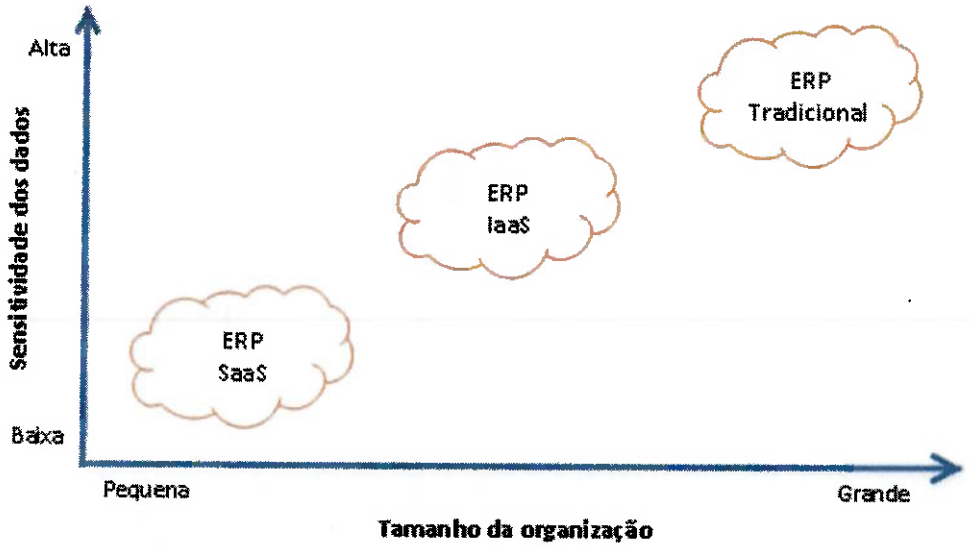

Figura 2.7 - Segurança X Tamanho da organização
Adaptado de [KIADEHI e MOHAMMADI, 2012]

Outro aspecto a ser considerado na escolha de um modelo de implementação é o tamanho da organização. A Figura 2.7 ilustra o cenário recomendado com base

nesse critério, combinado com o quão os dados tratados são sensíveis. Quanto maior a importância e segurança dos dados e maior o tamanho da organização, a utilização do ERP no modelo SaaS se torna menos recomendada. Neste caso, o ERP em ambiente próprio pode ser uma melhor opção.

Já a Figura 2.8 ilustra o mesmo cenário, mas com base no investimento necessário em combinação com a sensitividade dos dados tratados. Caso a organização procure uma maior segurança nos dados, é recomendada a utilização de um ERP em ambiente próprio, o que consequentemente eleva os custos com a implementação do ERP.

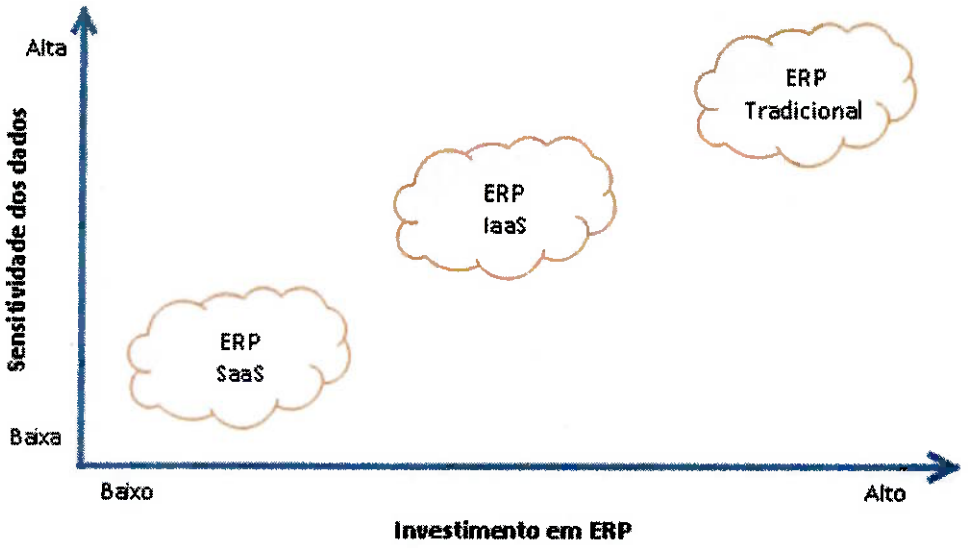

Figura 2.8 - Segurança X Investimento em ERP
Adaptado de [KIADEHI e MOHAMMADI, 2012]

Portanto, a decisão na escolha de cada cenário depende do nível de segurança e privacidade desejado, o tamanho da organização e de quanto a organização está disposta a investir na implementação do ERP, seja ele em ambiente próprio ou na nuvem.

3 Segurança na Computação em nuvem

Na computação tradicional, na qual toda a infraestrutura fica em ambientes próprios, a equipe de TI tem total controle sobre os dados da empresa, sabendo exatamente onde eles ficam armazenados e quem tem acesso aos mesmos. Em contrapartida, na computação em nuvem, todos os dados ficam armazenados no provedor de serviços. Nesse contexto a equipe de TI desconhece onde os dados estão sendo armazenados ou quem tem acesso aos mesmos, ou seja, a empresa passa a ter uma "perda de governança". Dessa maneira, surge a questão de como exigir garantias de que as informações armazenadas na nuvem estão realmente seguras [CASTRO e SOUSA]. Para solucionar este problema, deve-se analisar atentamente os contratos de prestação de serviços dos diversos provedores de computação em nuvem e também o Acordo de Nível de Serviço, conhecido pela sigla em inglês SLA (*Service Level Agreement*), que são voltados a garantir requisitos mínimos de qualidade e garantias de que possíveis incidentes não tragam grandes prejuízos aos clientes da nuvem [CASTRO e SOUSA] [ENISA].

Embora o SLA seja essencial para obter alguma garantia de segurança, cabe notar que a migração dos dados de uma empresa para a nuvem pode despertar interesses por parte de hackers, que podem tentar invadir o ambiente e fazer a coleta de dados para possível extorsão ou até mesmo visando a venda das informações a concorrentes. Portanto, embora provedores de serviços em nuvem afirmem com frequência que estão fazendo o possível para proteger os dados de seus clientes, ainda assim os dados na nuvem podem ser comprometidos. Tais preocupações podem ser observadas em uma pesquisa com 244 executivos da área de TI sobre os serviços oferecidos pela computação em nuvem [VELTE, VELTE e ELSENPETER, 2010]. Organizada pelo IDC (*International Data Corporation*), uma renomada empresa de pesquisa de mercado norte-americana na área de tecnologia da informação, a pesquisa mostrou que o item "segurança" continua sendo a maior preocupação entre os entrevistados (veja Figura 3.1).

Embora essa preocupação com a segurança da nuvem seja altamente relevante, é importante ressaltar que esse não é um problema exclusivo dessa

tecnologia, de modo que a migração de sistemas para a nuvem pode levar a um maior nível de segurança do que o obtido usando uma infraestrutura de TI tradicional. De fato, diversas empresas (em especial pequenas e médias) geralmente não possuem uma área de TI com especialistas em segurança e, portanto, sozinhas elas não são capazes de garantir a integridade dos dados em ambiente próprio. Já com a migração dos dados para nuvem, que são ambientes teoricamente com níveis de segurança superiores devido à presença de equipes mais bem preparadas, os dados dessas empresas estariam potencialmente mais protegidos a um custo de investimento bem menor.

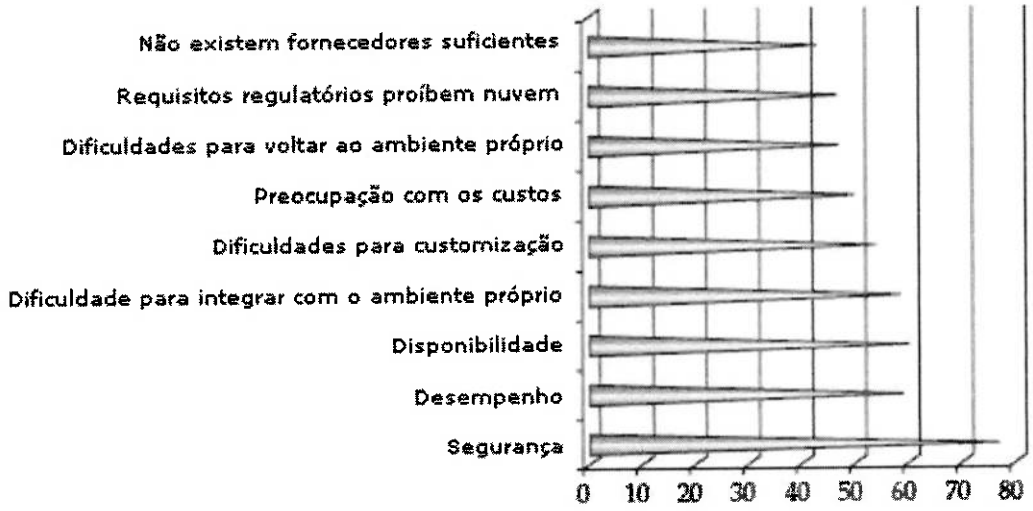

Figura 3.1 - Resultados da pesquisa IDC sobre as preocupações de segurança
Adaptado de [VELTE, VELTE e ELSENPETER, 2010]

Portanto, para obter maior benefício da tecnologia em nuvem, é importante entender seus prós e contras, tema este que é o principal objetivo do presente capítulo. Assim, as seções a seguir visam a discutir os benefícios relacionados à computação na nuvem e também os pontos que necessitam de um cuidado extra.

3.1 Benefícios

Conforme discutido anteriormente, provedores de serviços de nuvem em geral se preocupam em fornecer aos seus clientes um ambiente seguro, de modo a garantir a atratividade de seus serviços. Alguns dos potenciais benefícios de

segurança obtidos com o uso da nuvem são [VELTE, VELTE e ELSENPETER, 2010]:

3.1.1 Dados logicamente centralizados

Na infraestrutura de nuvem os dados da organização ficam logicamente centralizados, embora fisicamente distribuídos. Muito se fala do perigo de ter seus dados em apenas um local físico, algo comum em empresas de pequeno e médio porte. Assim, algumas boas características de segurança desse tipo de ambiente logicamente centralizado acabam tornando o sistema particularmente mais seguro. Por exemplo, é mais fácil implementar em tais ambientes soluções de filtragem, gerenciamento de atualizações, blindagem de máquinas virtuais e *hypervisors* e gerenciamento de ameaças.

Ainda segundo a ENISA [ENISA], a centralização dos dados traz vantagens econômicas no que diz respeito a controle de acesso físico e também na aplicação de muitos processos relacionados à segurança.

3.1.2 Redução na perda/roubo dos dados

Diversas organizações oferecem computadores portáteis aos seus funcionários, que por sua vez armazenam diversas informações no disco rígido desses equipamentos. Se este equipamento for esquecido em algum local ou roubado, todos os dados pessoais e da organização localmente armazenados estarão expostos, a não ser que haja algum mecanismo de segurança que os protejam (e.g., criptografia de disco).

Com a computação em nuvem, as organizações podem controlar melhor o acesso aos seus dados, limitando a quantidade de informações que o usuário pode obter do servidor e, assim, diminuir o comprometimento das informações em caso de extravio do equipamento.

3.1.3 Monitoramento

Se os dados da organização estão na nuvem, é potencialmente mais fácil monitorar a segurança dos servidores se comparado com o ambiente próprio, onde existem vários servidores físicos distribuídos por diversas localidades (unidades). Apesar de o ambiente na nuvem também possuir servidores fisicamente distribuídos, até mesmo em outras jurisdições, isso é transparente para o cliente.

Embora a concentração dos recursos seja um risco maior no caso de uma invasão, já que todos os dados estão lá, é preferível se preocupar com apenas um local, ao invés de vários. [VELTE, VELTE e ELSENPETER, 2010]

3.1.4 Troca imediata em caso de falha

Caso os dados sejam comprometidos por algum erro ou falha, o servidor não precisa ficar parado até que seja descoberto o motivo. Os dados podem ser movidos rapidamente para outro servidor sem afetar perceptivelmente as atividades dos usuários.

3.1.5 Registro das transações

O registro de transações (*log*) muitas vezes é deixado de lado, mas na nuvem o registro das transações é melhorado com a utilização de técnicas mais avançadas. Por exemplo, dada a elevada disponibilidade de recursos na nuvem, pode ser configurado no servidor de banco de dados Microsoft SQL Server um nível de auditoria C2, que raramente é usado em servidores locais devido à queda de desempenho que ele acarreta.

3.1.6 Compilações seguras

No ambiente de nuvem, não é necessário a aquisição de softwares adicionais para proteção da rede, diferentemente dos modelos de computação tradicional. Na nuvem, essas ferramentas geralmente estão disponíveis para que as organizações desenvolvam seus sistemas no nível de segurança desejado.

Além disso, todas as atualizações e testes podem ser feitos com base em uma imagem do servidor de produção em um ambiente desconectado, verificando que

alterações feitas não prejudiquem a operação da rede antes de colocá-las em produção.

3.1.7 Melhoria de segurança do software

Os fornecedores de software de segurança costumam incluir mecanismos cada vez mais avançados em suas aplicações. Neste contexto, é comum que os provedores de serviços na nuvem ajustem e atualizem a segurança de seus ambientes com uma frequência maior do que fazem clientes em seus próprios ambientes.

3.1.8 Testes de segurança

Os fornecedores de serviços do modelo SaaS e PaaS comumente realizam testes de segurança em suas aplicações e plataformas hospedadas. Por estarem em um ambiente compartilhado, embora os custos desses testes sejam elevados, os mesmos são divididos entre os inquilinos, de modo que o custo para o cliente acaba sendo menor do que o normalmente cobrado para tais serviços.

3.2 Riscos

Segundo a ENISA (*European Network and Information Security Agency*) [ENISA], o risco da utilização de computação em nuvem está relacionado diretamente com a oportunidade de negócio e o apetite pelo risco, ou seja, às vezes o risco é compensado pela oportunidade. Efetuando-se uma análise comparativa entre os dois ambientes (próprio x na nuvem), pode-se concluir que o risco é similar para ambos. Considere, por exemplo, uma planilha de cálculo. Se armazenada em ambiente próprio, ela pode ser compartilhada por correio eletrônico entre vários colaboradores. De modo semelhante, se for armazenada na nuvem ela também pode ser acessada por várias pessoas, sendo que a única diferença é que no ambiente próprio ela será armazenada em vários locais (estações de trabalho de cada usuário colaborador e no servidor), enquanto no ambiente de nuvem seu armazenamento é feito em apenas um local.

Ainda segundo a ENISA [ENISA], é possível para o cliente de nuvem transferir os riscos para o provedor do serviço. Entretanto, nem todos os riscos podem ser transferidos: se um risco leva ao fracasso do negócio, podem acontecer sérios danos ou implicações legais, sendo difícil ou impossível para qualquer uma das partes compensar tal dano. Entretanto, o cliente da nuvem costuma ser a entidade mais prejudicada, tendo em vista de que ele é o proprietário e, portanto, o maior interessado nos dados (muitas vezes confidencias).

Um estudo realizado pela ENISA [ENISA] identificou a relação entre a probabilidade e o impacto dos riscos na computação em nuvem, conforme mostra a Figura 3.2. Nesse estudo os riscos foram identificados e divididos em três categorias (Riscos Políticos e Organizacionais, Riscos Técnicos e Riscos Legais), e então representados em tabelas considerando: nível de probabilidade do risco, nível de impacto do risco, vulnerabilidades ocasionadas pelo risco, recursos afetados pelo risco e o nível do risco resultante. Os resultados são discutidos em maiores detalhes a seguir. Para o leitor interessado, as tabelas completas com esses dados encontram-se no APÊNDICE I – Tabelas de análise de riscos da computação em nuvem.

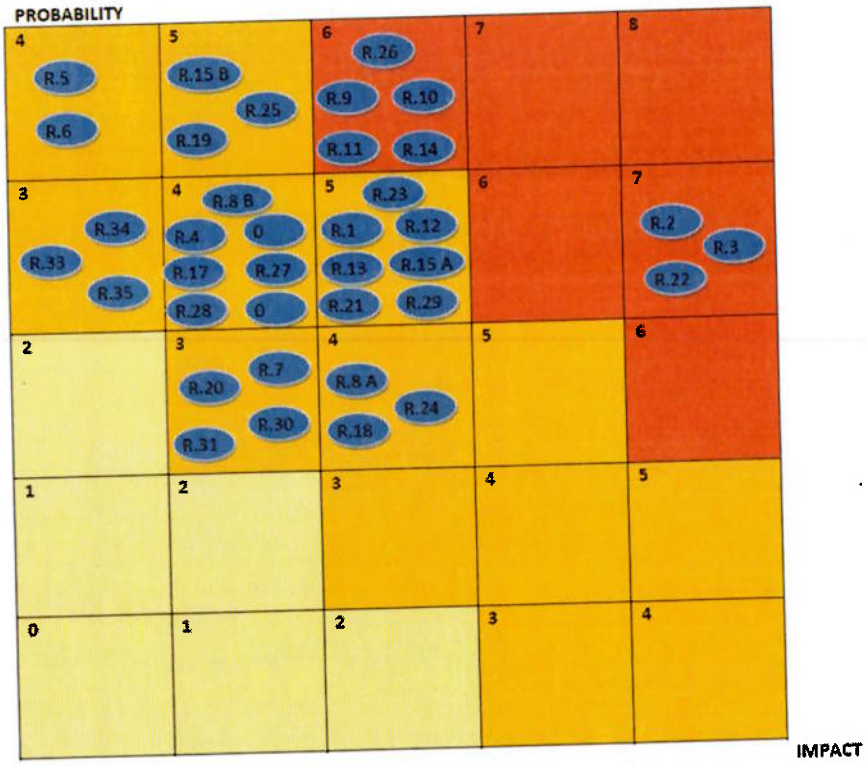

Figura 3.2 - Distribuição dos Riscos

Extraído de [ENISA]

3.2.1 Riscos políticos e organizacionais

As organizações atualmente possuem processos bem definidos e adequados aos modelos de computação tradicionais. Com a mudança para computação em nuvem, as organizações devem estar cientes de que esta mudança de tecnologia irá implicar em mudanças na organização, nos seus processos e processos de terceiros.

Algumas dessas mudanças nem sempre são aceitas, expondo assim a organização a riscos. Alguns destes riscos são discutidos a seguir:

3.2.1.1 Dependência de Fornecedor (Vendor Lock-in) – R1

A falta de padrões entre os fornecedores de serviços na nuvem pode gerar uma dependência do cliente com o seu fornecedor, dificultando a portabilidade de dados e serviços, ou até mesmo a migração do seu ambiente próprio para a nuvem. Além desta falta de padrões, os fornecedores podem, direta ou indiretamente, criar algumas dificuldades para impedir tal migração, como por exemplo: a cobrança de elevadas taxas por esse tipo de serviço. As restrições pertinentes a esse tipo de risco variam de acordo com cada modelo de serviço (SaaS, PaaS e IaaS), e são discutidas a seguir.

No modelo SaaS, cada fornecedor armazena as informações dos clientes em um modelo de banco de dados (tabelas, procedimentos armazenados, gatilhos, etc) próprio. Portanto, é muito difícil que os dados armazenados em um fornecedor sejam totalmente compatíveis com o futuro fornecedor. É oferecido ao cliente a opção de exportação dos dados em algum formato padrão, por exemplo, arquivos XML. Porém, nem sempre essa alternativa é oferecida, de modo que cabe ao cliente negociar com o fornecedor o desenvolvimento de uma ferramenta para efetuar a exportação dos dados.

No modelo PaaS, o problema está relacionado com as APIs (*Application Programming Interface*) de cada fornecedor. Por exemplo, as chamadas desenvolvidas para acesso à API de um fornecedor podem ser diferentes daquelas que devem ser utilizadas para o futuro fornecedor. Deste modo, o código

desenvolvido pode não ser portável. Como resultado, da mesma maneira que acontece no SaaS, cabe ao cliente arcar com os custos da migração.

No modelo IaaS, o fornecedor para qual o cliente deseja fazer a migração pode utilizar um modelo de máquina virtual diferente do fornecedor atual. Apesar de a maioria dos fornecedores utilizarem máquinas virtuais baseadas em *hypervisors* de padrões conhecidos ou mesmo abertos, a migração entre fornecedores pode não ser uma tarefa muito simples.

Apesar de os riscos relativos a dependência de fornecedores serem relevantes a qualquer tipo de software, tais preocupações têm especial relevância no que se refere a aplicações críticas, como ERPs. Portanto, na contratação de um ERP na nuvem, deve-se levar em consideração a reputação do provedor. Deve-se também optar pela contratação de provedores que possuam interfaces para migração de dados de ERP de outros fabricantes.

3.2.1.2 Perda de governança – R2

Quando uma empresa faz a escolha de mudar sua infraestrutura para a nuvem, ela deixa de ter o controle completo sobre seus dados, passando os mesmos para o fornecedor da nuvem. Assim, uma série de questões relativas à segurança são afetadas. Um exemplo disso é o contrato de "Termos de Uso" que podem proibir testes de vulnerabilidades e invasão dos ambientes por parte do cliente da nuvem.

Outro risco da perda de governança é o fato de que o fornecedor da nuvem pode subcontratar serviços de terceiros. Por exemplo: o enlace de dados pode ser fornecido por um provedor de rede que não oferece as mesmas garantias do fornecedor da nuvem. Sendo assim, os dados dos clientes correm o risco de ficarem expostos.

No contexto de ERPs, da mesma forma que o item anterior, deve-se levar em consideração a reputação do provedor. Provedores com melhor reputação tendem a ter procedimentos bem definidos que atendam aos requisitos de governança, auditorias, entre outros.

3.2.1.3 Desafios relacionados à conformidade – R3

Muitas das empresas que estão migrando seu ambiente para a nuvem têm investido fortemente na obtenção de certificações para se adequar aos padrões de segurança na proteção dos dados. Um exemplo deste tipo de certificação é o PCI-DSS (*Payment Card Industry - Data Secutity Standart*) que especifica as recomendações mínimas e obrigatórias relativas à segurança de sistemas de pagamento, como sistemas baseados em cartões de crédito, por exemplo [PCI].

Todo este investimento pode ser posto em risco se o provedor da nuvem não comprovar a sua própria conformidade com os requisitos aplicáveis e/ou se ele não permitir que o seu cliente efetue auditoria para avaliar a sua aderência aos requisitos de segurança. Por outro lado, clientes de serviços de infraestrutura de nuvem pública, com por exemplo o Amazon EC2, têm tido dificuldade em obter a certificação PCI-DSS para este tipo de ambiente. Por essa razão, eles costumam ficar impossibilitados de utilizar sistemas com transações de cartão de crédito.

Diversos ERPs possuem módulos adicionais de comércio eletrônico, que possibilitam a venda de produtos via internet. Caso o fabricante deste módulo exija uma certificação PCI-DSS, a implementação do ERP pode ser comprometida.

3.2.1.4 Perda de reputação devido a atividades de outros clientes – R4

Ter os recursos compartilhados com outros inquilinos pode ser um risco caso algum dos inquilinos decida fazer alguma atividade maliciosa. Por exemplo, o envio de SPAM (*Sending and Posting Advertisement in Mass*) ou o fornecimento de conteúdo malicioso pode acarretar no bloqueio de um intervalo de endereços IP (*Internet Protocol*), possivelmente prejudicando todos que compartilham do mesmo recurso.

Em consequência disso, o cliente pode ter sua reputação prejudicada incorretamente, ou até mesmo ser vítima de perda de dados caso a ação indevida de outro inquilino ocasione o confisco do hardware pelas autoridades.

Tal questão pode ser aplicada a qualquer software que utilize ambiente da nuvem, mas o problema se agrava em aplicações críticas, como ERPs. Isto ocorre porque aplicações ERP possuem informações confidenciais de clientes e

fornecedores, faturamento da empresa, entre outros. Assim, a exposição dessas informações a terceiros podem prejudicar a organização.

3.2.1.5 Encerramento das atividades ou falhas por parte do provedor – R5

A elevada concorrência, uma estratégia inapropriada ou até mesmo a falta de capacidade financeira podem levar à falência de um provedor de serviços na nuvem. Até que o cliente transfira seus dados para outro provedor, ele corre o risco de ficar com o serviço fora do ar ou necessitar de investimentos adicionais para efetuar a migração.

Além disso, qualquer falha na prestação de serviço pelo provedor de nuvem ou nos serviços de terceiros prestados a este último também podem prejudicar os clientes do serviço.

A indisponibilidade de aplicações críticas (e.g., ERPs), mesmo que por alguns instantes, pode acarretar grandes prejuízos para a organização. O ideal é que a organização possua um plano de contingência para evitar maiores perdas. Esta preocupação também vale para outros tipos de sistemas.

3.2.1.6 Negociação entre fornecedores – R6

A negociação entre provedores de serviços de nuvem pode afetar diretamente os interesses dos clientes. Por exemplo, em caso de aquisições, o provedor que está adquirindo o controle sobre o outro pode não ter as mesmas políticas de segurança, acordos de SLA, entre outros, ocasionando um impacto direto nos requisitos de segurança dos clientes.

No contexto de ERPs, assim como em qualquer outra aplicação, essa questão deve ser analisada como uma nova contratação, ou seja, todas as precauções adotadas na aquisição do provedor de nuvem devem sem tomadas para garantir a segurança.

3.2.1.7 *Falha da cadeia de fornecimento – R7*

Conforme discutido anteriormente, um provedor de nuvem pode terceirizar alguns serviços ou tarefas para outras empresas. Assim, o nível de segurança do fornecedor depende diretamente no nível de segurança de cada terceiro contratado. Qualquer falha por parte deste pode acarretar em diversos problemas, tais como: indisponibilidade, perda de confidencialidade, integridade e disponibilidade, violação de SLA, entre outros.

É de extrema importância que o provedor deixe bem claro no contrato de prestação de serviços qual ou quais serviços e tarefas são terceirizados. Além disso, é importante que ele também comunique aos clientes quando algum dos terceiros for substituído por outro. Só assim o cliente poderá avaliar adequadamente qual o risco que ele estará correndo.

3.2.2 Riscos Técnicos

Os riscos técnicos estão diretamente relacionados aos problemas tecnológicos que as organizações podem encontrar ao migrar os dados e aplicações para ambientes na nuvem. Tais riscos incluem a interceptação dos dados por terceiros, novas tecnologias, entre outros.

3.2.2.1 *Falta de recursos – R8*

Por se tratar de um ambiente com serviços sob demanda, os recursos são alocados de acordo com cálculos em projeções estatísticas. Um dimensionamento de recurso inadequado para menos pode acarretar em indisponibilidade do serviço, ocasionando prejuízos para a organização. Já um dimensionamento de recurso inadequado para mais irá gerar um custo excessivo e desnecessário para o provedor, que pode ser repassado para o cliente.

3.2.2.2 *Isolamento a falhas – R9*

É comum em ambientes de nuvem, principalmente em nuvens públicas, o compartilhamento de recursos de hardware. Falhas nos mecanismos de isolamento de recursos de armazenamento, memória e roteamento podem expor dados de outros inquilinos que compartilham do mesmo ambiente no caso de um ataque (e.g.: *SQL Injection*).

Esta preocupação, apesar de aplicável a qualquer sistema, requer uma atenção especial em aplicações críticas, como ERPs. Aplicações ERPs geralmente utilizam-se de banco de dados para armazenamento das informações. Se um cliente conseguir acessar o banco de dados de outro cliente, e os dados não forem criptografados, a segurança estará comprometida.

3.2.2.3 *Funcionários maliciosos por parte do provedor – R10*

Administradores, auditores e prestadores de serviços têm papéis considerados de alto risco dentro de um provedor de nuvem, pois eles muitas vezes possuem acesso irrestrito (dependendo do papel) a dados privilegiados. Qualquer atividade maliciosa por parte destes atores pode comprometer a confidencialidade e a integridade dos dados, comprometendo assim a reputação da organização e a confiança do cliente.

3.2.2.4 *Interfaces de administração vulneráveis – R11*

Geralmente, a administração dos recursos em ambientes de nuvem é feita via Internet, através de navegadores web ou via software de acesso remoto. Se o provedor de serviços não fizer um forte investimento em segurança, as vulnerabilidades dos navegadores ou programa de acesso remoto podem comprometer os dados da empresa.

Além disso, o risco pode ser ainda maior caso o provedor de serviços também utilize-se dessas interfaces para fazer o gerenciamento da nuvem. Este é o caso ilustrado na Figura 3.3, onde todo o gerenciamento dos clientes de uma aplicação ERP na nuvem é feito através de uma interface web. Se um invasor tiver acesso a

essa interface, todos os clientes que compartilham desse ambiente serão potencialmente prejudicados.

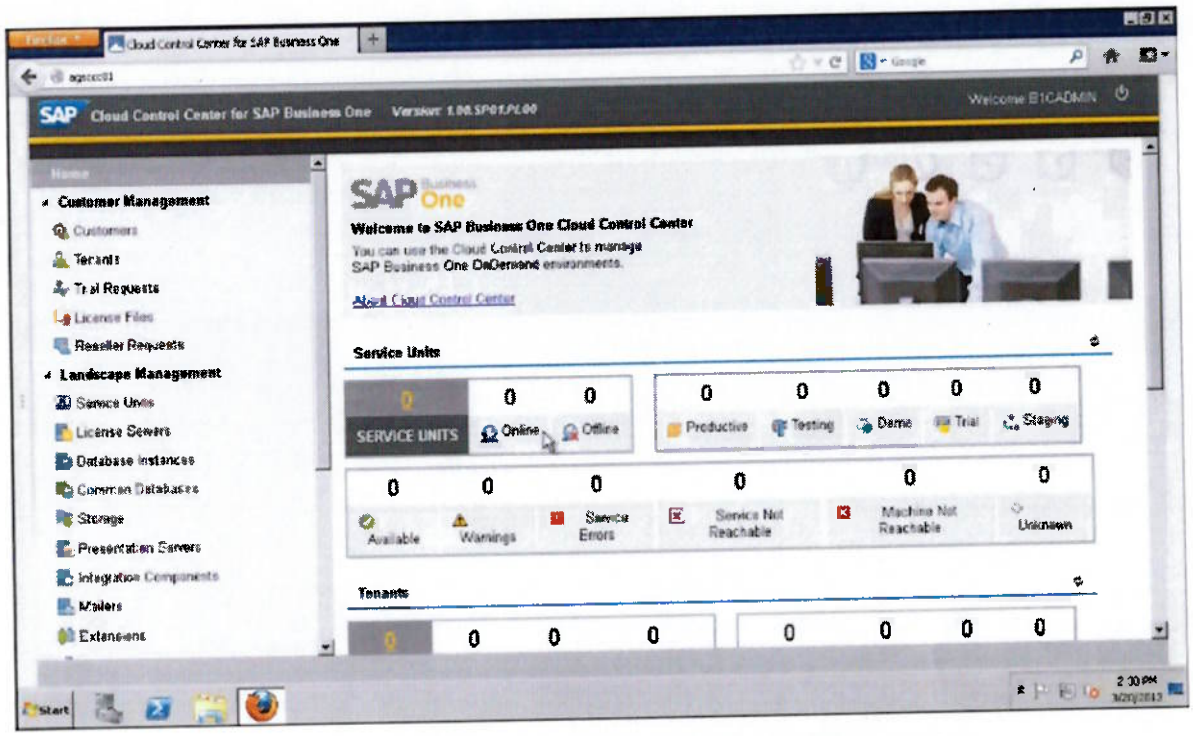

Figura 3.3- Interface web de administração do ERP na nuvem

3.2.2.5 Interceptação de dados em trânsito – R12

Se comparado com ambientes tradicionais, onde os servidores ficam em ambientes próprios (dentro da própria empresa), a computação em nuvem tem uma quantidade de dados muito maior trafegando pela rede. Isso pode ser um risco se esses dados forem interceptados durante a transferência entre nuvens ou durante o acesso a alguma aplicação pelos usuários.

Um exemplo desse risco em aplicações ERP é o fato de, durante o acesso feito por um usuário na aplicação, dados de clientes, custos de produtos, faturamento da organização, entre outros, podem ser interceptados por terceiros. Dependendo no nível da informação coletada, pode-se levar a organização à falência por meio de concorrência desleal ou mesmo via ações legais.

Outras fontes de ameaça são: captura de tráfego (*sniffing*), falsificação de endereços (*spoofing*), ataque de personificação do tipo "homem no meio" (*man-in-the-middle*), ataque por canal secundário (*side channel*) e ataque de repetição (*replay*).

3.2.2.6 Vazamento de dados no upload/download – R13

Da mesma forma que o risco anterior, este risco se aplica na transferência de dados entre o provedor da nuvem e seu cliente. Na implementação de um ERP, por exemplo, grandes quantidades de dados são transmitidas, geralmente através de arquivos XML para dar carga inicial ao sistema, permitindo a concretização de tais ataques.

3.2.2.7 Eliminação de dados insegura ou ineficiente – R14

A menos que alguma forma de criptografia de dados ou outra técnica efetiva de proteção seja utilizada, é praticamente impossível garantir que os dados não estejam em risco mesmo após sua remoção. Como a destruição física do disco rígido é geralmente impossível de ser realizada nesses casos, deve-se efetuar testes de recuperação de dados a fim de identificar qualquer resíduo que possa comprometer a organização. Caso contrário, os dados podem estar expostos a terceiros.

Embora esse risco se aplique a todos os sistemas, novamente as aplicações críticas, como os ERPs, requerem um maior cuidado no descarte dos dados: por trabalharem com informações confidenciais, elas necessitam de uma garantia que realmente todos os dados foram excluídos.

3.2.2.8 Distributed Denial of Service (DDoS) – R15

Ataques distribuídos de negação de serviço são uma variação dos ataques de DoS (*Denial of Service* ou Negação de Serviço), que consistem no envio (por parte do atacante) de uma grande quantidade de pacotes a fim de ocasionar uma parada

temporária dos serviços. Nos ambientes de nuvem, que possuem uma infraestrutura compartilhada entre um ou mais clientes, o potencial deste tipo de ataque é muito maior se comparado com o modelo de computação tradicional.

Muitas das medidas para proteção desse tipo de ataque não são eficazes, pois, normalmente, não é possível efetuar uma distinção entre tráfego legítimo e de ataque se este último não possuir uma assinatura ou não puder ser identificado como malicioso. O problema pode se tornar ainda mais grave se o ataque for efetuado usando uma *botnet* (conjunto de computadores comprometidos). [SABAHI, 2011]

3.2.2.9 Economic Denial of Service (EDoS) – R16

A exemplo do DDoS, este tipo de ataque é uma variante do DoS. Porém, ao contrário do caso anterior, que consiste em ocasionar uma falha no serviço, este tipo de ataque visa prejudicar financeiramente uma organização que possua seus recursos na nuvem.

Conforme mencionado anteriormente, na computação em nuvem o cliente tem a possibilidade de pagar apenas pelos recursos utilizados ("*pay-as-you-go*"). Ao receber um ataque de negação de serviço, o consumo de recursos irá aumentar consideravelmente, tendo impacto direto nos custos da contratação. O problema pode se agravar especialmente caso o cliente da nuvem não configure os limites de utilização dos recursos.

3.2.2.10 Exposição da chave de criptografia – R17

A exposição de chaves secretas ou senhas para pessoas mal intencionadas são um risco para as organizações, pois podem permitir acesso não autorizado ou interceptação de dados em sessões SSL (*Secure Sockets Layer* -- Protocolo de Camada de Sockets Segura), arquivos cifrados, etc.

3.2.2.11 Realização de varredura e sondagens maliciosas– R18

Os testes de varreduras e sondagens maliciosas, como também o mapeamento da rede, são considerados ameaças indiretas aos recursos disponibilizados na nuvem. Isso porque tais ameaças são utilizadas apenas para a obtenção de informações do ambiente em questão, como por exemplo, serviços e portas utilizadas, quantidade de computadores na rede, etc. A ameaça passa a ser direta quando o mapeamento de todo o ambiente é concluído e o invasor tem condições de realizar um ataque assertivo. As informações coletadas por este tipo de atividade facilitam ataques que acarretariam em uma perda de confidencialidade, integridade e disponibilidade dos serviços e dados.

3.2.2.12 Plataformas vulneráveis – R19

No modelo de serviço IaaS, por exemplo, é comum os provedores de nuvem utilizarem um *hypervisor* como componente base da plataforma de virtualização. Como qualquer outra camada de software, esta plataforma também pode ter vulnerabilidades, estando propensa a ataques ou falhas inesperadas.

3.2.2.13 Conflitos entre os processos de segurança do cliente e da nuvem – R20

Os provedores de serviços em nuvem devem definir uma separação muito clara das responsabilidades que os clientes devem ter ao contratar os serviços de nuvem. Uma falha por parte do cliente pode comprometer toda a plataforma da nuvem caso o provedor não tenha tomado todas as medidas necessárias para garantir o seu isolamento. Portanto, os provedores de nuvem devem fornecer aos clientes um guia de melhores práticas para garantir a proteção dos seus recursos.

Alguns clientes de nuvem têm a impressão incorreta de que o provedor de nuvem é o único responsável por garantir a segurança e proteção dos dados. Se o provedor de nuvem não informar ao cliente de forma clara esta divisão de responsabilidades, o ambiente corre riscos desnecessariamente.

3.2.3 Riscos Legais

A entrega de serviços de nuvem pode ser feita em qualquer lugar do planeta, ou seja, ao adquirir esse tipo de serviço, os dados de uma empresa podem estar fora do território nacional. Diferentemente dos modelos de computação tradicional, no qual as leis aplicadas se baseiam em leis locais, na computação em nuvem geralmente as leis aplicadas são as leis do país onde os dados estão localizados.

Portanto, o consumidor de serviços na nuvem deve atentar-se a este detalhe para não ter problemas futuros ao armazenar seus dados fora do país. [COMPUTERWORLD]. A seguir são detalhados alguns desses riscos:

3.2.3.1 Intimação e confisco de hardware – R21

Conforme mencionado anteriormente, é comum o compartilhamento de hardware entre um ou mais inquilinos em um ambiente de nuvem. Se a atividade suspeita de algum inquilino acarretar no confisco do hardware físico pelas autoridades, os dados de todos os outros inquilinos que compartilham o mesmo hardware podem ser expostos indevidamente.

3.2.3.2 Riscos de mudanças de jurisdição – R22

Alguns provedores de serviços de nuvem podem distribuir os dados dos clientes entre diferentes jurisdições, sendo que algumas delas podem ser de alto risco. Existem países que são carentes de leis ou que possuem autoridades autocráticas ou até mesmo países que não respeitam acordos internacionais. Portanto, a qualquer momento, as autoridades desses países podem acessar (legal ou ilegalmente) os *datacenters* dos provedores e, assim como no item anterior, causar a exposição dos dados dos clientes indevidamente.

3.2.3.3 Riscos de proteção de dados – R23

Não é comum que os provedores de serviços de nuvem forneçam detalhes da coleta e manipulação de dados pessoais que eles realizam. Portanto, pode ser muito difícil para o cliente da nuvem verificar de forma eficaz se os dados que estão sendo coletados e manipulados pelo provedor estão sendo tratados de forma legal.

Neste contexto, deve ficar bem claro para o cliente da nuvem que ele é o principal responsável pelo tratamento dos dados pessoais, mesmo que esse trabalho seja executado pelo próprio provedor de nuvem. O não cumprimento das normas de proteção de dados pode acarretar punições administrativas, civis e penais previstas pela lei.

3.2.3.4 Riscos de licenciamento – R24

Dependendo do tipo de licença (licenças por servidor ou verificação de licença online), pode-se encontrar problemas no ambiente de nuvem. Por exemplo, se a licença de um software é cobrada por servidor, a cada nova instância criada os custos com licença serão aplicados, podendo acarretar em gastos elevados.

4 Estudo de caso: Aplicação ERP na nuvem

O estudo de caso apresentado neste capítulo tem como objetivo analisar uma aplicação ERP no ambiente de nuvem. Além disso, é realizada também uma análise comparativa dessa mesma aplicação com a aplicação em ambiente local.

Para este estudo foi escolhida a aplicação ERP SAP® Business One OnDemand, produzida e comercializada pela SAP AG. A aplicação é oferecida no modelo SaaS por parceiros credenciados pela SAP, mas também existe a possibilidade de instalação em nuvem privada. A motivação na escolha desta aplicação em específico se deve ao fato do autor do presente trabalho ter fácil acesso e familiaridade com a mesma.

4.1 Aplicação SAP tradicional *vs.* nuvem

O SAP é um ERP bastante utilizado em ambientes empresariais do mundo todo, embora apenas mais recentemente tenha surgido uma versão baseada em nuvem. Uma das principais diferenças da aplicação SAP tradicional em relação à aplicação SAP na nuvem, além do baixo custo de propriedade (TCO), está na instalação da aplicação. Na aplicação tradicional, a instalação precisa ser efetuada individualmente, em cada estação de trabalho. Já na aplicação na nuvem, ela é hospedada e mantida por terceiros e acessada geralmente através de um navegador web. [LEWANDOWSKI, SALAKO e GARCIA-PEREZ, 2013]

A seguir são discutidas e comparadas essas duas aplicações.

4.1.1 SAP® Business One (*local*)

O SAP® Business One é uma solução de gestão empresarial projetada especificamente para pequenas e médias empresas. A solução compreende diversas das funções básicas para aumentar o controle e automatização dos processos de negócio das organizações. São elas: administração, contabilidade financeira, serviços bancários, compras, vendas, gestão de relacionamento com

cliente – CRM (Customer Relationship Management), controle de estoque, manufatura, contabilidade gerencial e relatórios. A Figura 4.1 ilustra a ferramenta.

A solução reside em servidores com plataforma Microsoft® Windows® e banco de dados SQL Server da Microsoft®. A solução também oferece uma interface de programação de aplicativos baseada na tecnologia COM (*Component Object Model*), que permite aumentar o seu escopo funcional para atender a necessidades específicas do usuário.

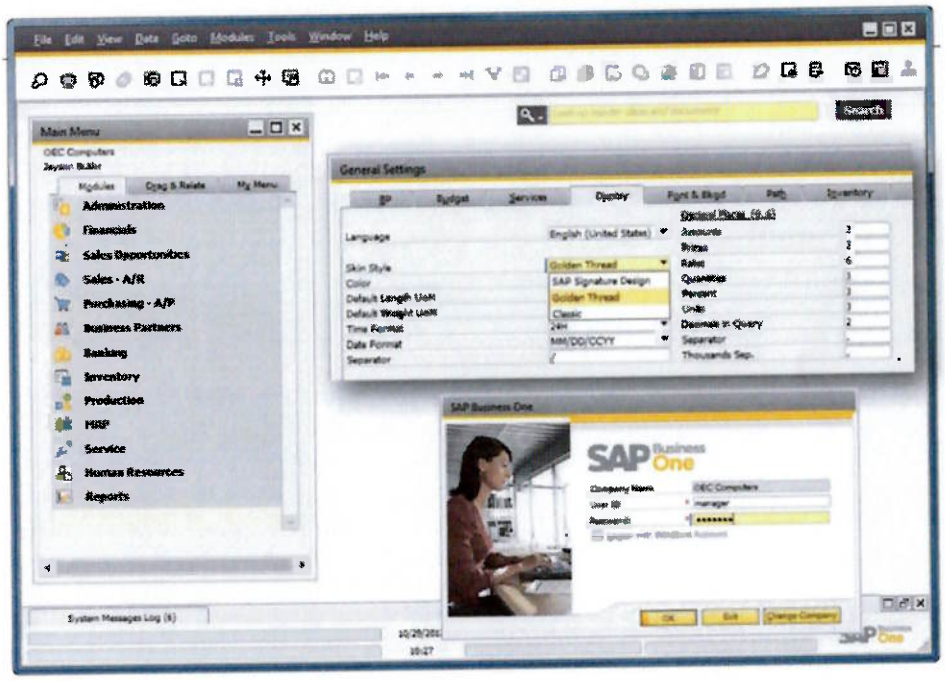

Figura 4.1 - Aplicação SAP® Business One

4.1.2 SAP® Business One OnDemand

O SAP® Business One OnDemand é a solução SAP® Business One baseada na nuvem. Todos os recursos e funcionalidades encontrados na solução local são disponibilizados através da nuvem, sendo que nesta última a organização paga uma taxa mensal pela sua utilização. A entrega (gerenciamento e hospedagem) é feita única e exclusivamente por parceiros SAP® credenciados.

A vantagem na utilização desse modelo de solução em nuvem em comparação a uma implementação local é uma menor complexidade e maior rapidez na implementação, além de um menor investimento. A manutenção e atualização é feita

automaticamente pelo parceiro SAP®, colocando à disposição da organização, assim, a tecnologia mais atual.

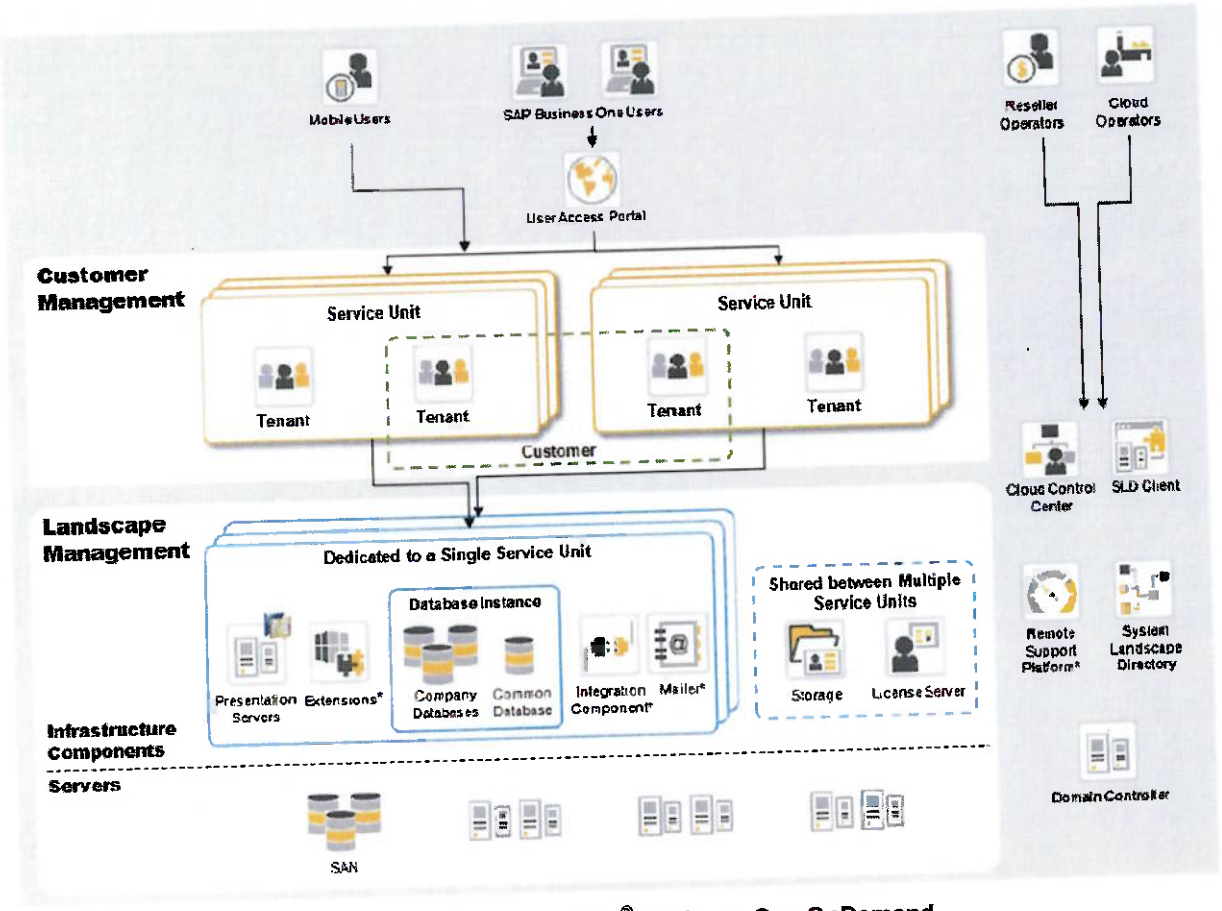

Figura 4.2 - Arquitetura SAP® Business One OnDemand

Extraído de [SAP Business One OnDemand]

A Figura 4.2 ilustra a arquitetura necessária para suportar a aplicação em questão. A arquitetura é composta por:

1. Servidores de apresentação (*Presentation Servers*): servidores onde são instalados os clientes da aplicação;
2. Banco de dados do *core* da aplicação (*Common Database*);
3. Bancos de dados de cada inquilino (*Company Database*): um mesmo inquilino pode possuir um ou mais banco de dados;
4. Componente de integração (*Integration Component*): responsável por efetuar a integração da aplicação com outras plataformas;
5. Extensões e aplicação de envio de e-mail;

6. Servidor de armazenamento (*Storage*): responsável por armazenar arquivos (anexos);
7. Servidor de licença (*License Server*).

A arquitetura listada acima pode ser compartilhada por um ou mais inquilinos. O acesso à aplicação por parte dos usuários é feito através de um portal web, conforme ilustra a Figura 4.3, ou utilizando a aplicação para dispositivos móveis.

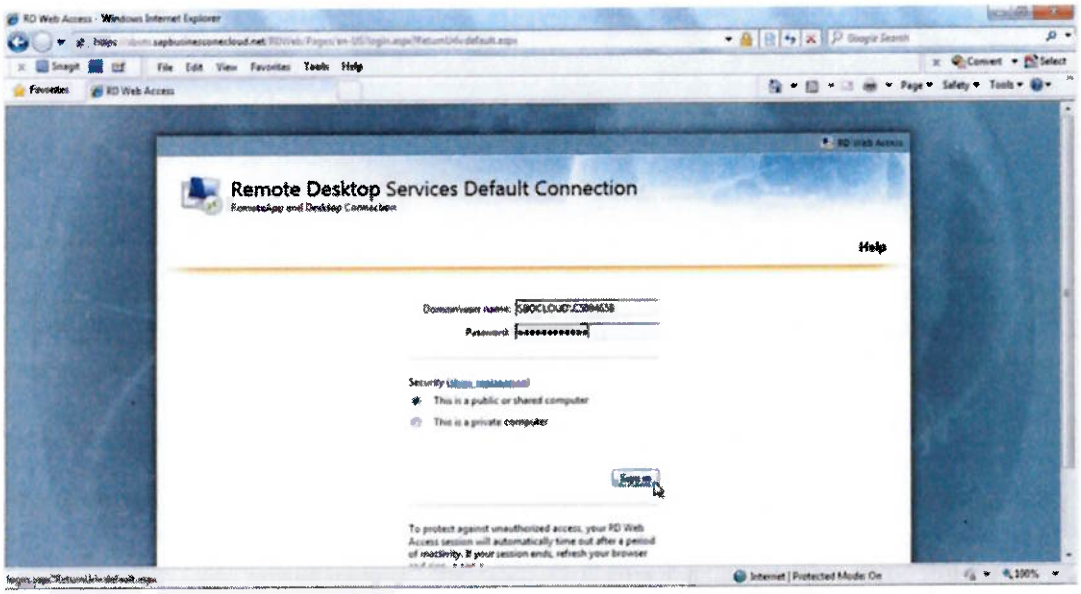

Figura 4.3 - SAP® Business One OnDemand - Portal de acesso web

4.1.3 Análise

Se o intuido da empresa é a redução de custos, a escolha pelo modelo IaaS em ambiente próprio acaba não sendo vantajosa, pois além dos custos com hardware já conhecidos na implementação de ERPs tradicionais, soma-se a aquisição de softwares para virtualização. Por outro lado, se for adotada a solução em ambiente SaaS a economia é significativa, pois não são mais necessários os custos com aquisição e manutenção de hardware e software. Por esta razão, o presente estudo considera apenas implementação neste último modelo.

Os custos referentes à aquisição e implementação das aplicações SAP® Business One OnPremise e SAP® Business One OnDemand, obtidos em consulta direta a empresa SAP, encontram-se na Tabela 4.1. Para a aplicação na nuvem, os valores fornecidos são para um contrato de 48 meses.

Conforme mostrado nessa tabela, para a aplicação tradicional, as licenças se dividem em 6 (seis) do tipo *Professional*, que dão acesso a todos os módulos da aplicação (dependendo apenas das permissões que lhe forem concedidas), e outras 9 limitadas a módulos específicos, a saber: 3 (três) do tipo *Limited Logistics*, 3 (três) do tipo *Limited Financials* e 3 (três) do tipo *Limited CRM*. Por exemplo, a licença *Limited Financials* dá direito de acesso apenas aos módulos Finanças e Banco (Contas a pagar e receber). Já para a aplicação na nuvem, todas as 15 (quinze) licenças são do tipo *Professional*.

Tabela 4.1 - Custos de implementação das aplicações SAP

	SAP® Business One OnPremise	SAP® Business One OnDemand
Número de licenças	15 (6 Professional + 9 Limited)	15 (todas Professional)
Valor total das licenças	R$ 129.800,00	R$ 2.086,17 (mensal)
Manutenção anual	R$ 28.571,00	Não possui
Valor de implantação (400 horas)	R$ 53.200,00	R$ 53.200,00
Total	R$ 211.571,00 (12 meses)	R$ 153.336,16 (48 meses)

Dos valores financeiros destacados na Tabela 4.1, pode-se notar que de fato a aplicação tradicional é consideravelmente mais custosa, e dificilmente seria escolhida se a opção da empresa for a redução de custos. De fato, na tabela em questão não estão inclusos os valores referentes a aquisição de hardware e software (sistema operacional e banco de dados) para instalação do servidor da aplicação tradicional, o que aumentaria ainda mais os custos envolvidos. Já na aplicação SAP® Business One OnDemand, por ser uma aplicação na nuvem, o modelo de pagamento é o "*pay-as-you-go*". Isto pode ser uma vantagem com relação a gerenciamento de custos, já que a empresa não tem que pagar o valor total da aplicação logo no início do projeto, que é o caso da aplicação no modelo tradicional. Por outro lado, sendo esta uma licença do tipo locação, ao final do contrato ou até mesmo se o cliente cancelar o mesmo, ele perde o acesso ao

sistema. Já na aplicação SAP® Business One tradicional, mesmo se o cliente cancelar o contrato ele continua tendo acesso ao sistema, deixando apenas de receber suporte, manutenção e atualizações do produto.

5 Considerações Finais

A computação em nuvem pode ser uma boa aliada das organizações que buscam a redução de custo em TI. Neste trabalho foram apresentados alguns dos benefícios na utilização desse tipo de ambiente, bem como diversos pontos que as organizações devem analisar para evitar problemas com a utilização de serviços em nuvem. Especificamente, foram listados diversos dos riscos que devem ser levados em consideração quando se adota o modelo em nuvem.

Apesar de a segurança dos dados ser um dos itens de maior preocupação das organizações ao migrar seus dados para a nuvem e uma das motivações para o desenvolvimento deste trabalho, a literatura mostra que, para pequenas e médias empresas buscando a redução de custos na implementação de um ERP na nuvem, a segurança dos dados muitas vezes não é a maior preocupação se comparada com os tradicionais problemas de um ERP, como a impossibilidade de personalização, desempenho e integração com outros sistemas. Por outro lado, embora os custos de implementação e utilização de um ERP na nuvem sejam bem menores do que os de um ERP tradicional, conforme foi mostrado no estudo de caso deste trabalho, o cliente não obtém propriedade sobre a aplicação. Assim, ao término do contrato, nenhuma parte do valor investido na aplicação é devolvido, o que torna difícil a utilização de um ERP na nuvem principalmente a longo prazo.

Portanto, cada empresa deve avaliar o nível de segurança desejado e o quanto está disposta a investir em um ERP antes de partir para uma abordagem baseada em nuvem.

5.1 Contribuições do Trabalho

O intuito deste trabalho foi reunir os diversos benefícios e riscos da computação em nuvem e relacioná-los à utilização de aplicações ERPs para este tipo de cenário, discutindo prós e contras que possam influenciar na decisão da escolha em se utilizar de ERPs em nuvem ou ambiente próprio.

5.2 Trabalhos Futuros

Por ser um tema relativamente recente, a computação em nuvem ainda não está totalmente madura, sendo uma tecnologia que encontra-se em constante evolução. Este trabalho focou principalmente aspectos de segurança, mas existem várias outras vertentes para serem estudadas. Portanto, como trabalhos futuros, este trabalho pode ser estendido por meio de estudos sobre o desempenho de aplicações na nuvem comparados com as aplicações instaladas localmente.

6 Referências

[AMAZON] Regiões e Zonas de disponibilidade. **Amazon EC2**. Disponivel em: <http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html>. Acesso em: Outubro 2013.

[CASTRO, R.; SOUSA, V.]. **Segurança em Cloud Computing - Governança e Gerenciamento de Riscos de Segurança.** Dissertação (Mestrado Profissional em Computação) - Instituto Federal de Educação, Ciência e Tecnologia do Ceará, Universidade Estadual do Ceará, Ceará.

[CHOPRA, S.; MEINDL, P.] **Gerenciamento da Cadeia de Suprimentos:** Estratégia, Planejamento e Operação. 1ª Ed. ed. [S.l.]: Pearson, 2002.

[COMPUTERWORLD] Conheça os riscos legais de cloud computing. **COMPUTERWORLD**. Disponivel em: <http://computerworld.com.br/negocios/2011/11/17/conheca-os-riscos-legais-de-cloud-computing/>. Acesso em: Janeiro 2014.

[ENISA]. **Benefits, risks and recommendations for information security**. Novembro, 2009.

[KIADEHI, E.; MOHAMMADI, S.]. **Cloud ERP - Implementation of Enterprise Resource Planning Using Cloud Computing Technology**, 2012. TextRoad Publication.

[LEWANDOWSKI, J.; SALAKO, A. O.; GARCIA-PEREZ, A.] SaaS Enterprise Resource Planning Systems: Challenges of their adoption in SMEs. **IEEE**, 2013. 10th IEEE International Conference, p. 56-61.

[MAUSER, D.; DIOGENES, Y.] **Certificação Security - da Prática Para o Exame Syo-301**. 2ª. ed. [S.l.]: Novaterra, 2013.

[MELL, P.; GRANCE, T.] The NIST Definition of Cloud Computing. **NIST**, 2011. NIST Special Publication 800-145, 7p. Disponivel em: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.

[PCI] PCI SSC Data Security Standards Overview. **PCI**. Disponivel em: <https://www.pcisecuritystandards.org/security_standards/>. Acesso em: Novembro 2013.

[RAINES, G.] MITRE Corporation. **Cloud Computing and SOA**, 2009.

[SABAHI, F.] IEEE. **Cloud Computing Security Threats and Responses**, 2011. 3rd IEEE International Conference, p. 245-249.

[SAP Business One OnDemand]. **SAP AG**. Disponivel em: <http://www.sap.com/solution/sme/software/erp/small-business-management/cloud/index.html>. Acesso em: Setembro 2013.

[VELTE, A.; VELTE, T.; ELSENPETER, R.] **Computação em Nuvem - Uma Abordagem Prática**. Rio de Janeiro: Alta Books, 2010.

[VERAS, M.] **Virtualização - Componente Cental do Datacenter**. 1ª Ed. ed. Rio de Janeiro: Brasport, 2011.

7 APÊNDICE I – Tabelas de análise de riscos da computação em nuvem

As tabelas listadas abaixo complementam os riscos discutidos no Capítulo 3.2. Cada risco apresentado nas mesmas inclui: probabilidade do risco, impacto do risco, vulnerabilidades, recursos afetados e o nível do risco.

Tabela 7.1 - Riscos políticos e organizacionais - Dependência de fornecedor (R1)

Adaptado de [ENISA]

Probabilidade	Alta
Impacto	Médio
Vulnerabilidades	V13. Falta de tecnologias e soluções padrão V31. Falta de integridade e transparência nos termos de uso V46. Má escolha de provedor V47. Falta de redundância do fornecedor
Recursos afetados	A1. Reputação da empresa A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.2 - Riscos políticos e organizacionais - Perda de governança (R2)

Adaptado de [ENISA]

Probabilidade	Muito alta
Impacto	Muito alto (dependendo da organização) (IaaS – Muito alto, SaaS – Baixo)
Vulnerabilidades	V34. Papéis e responsabilidades pouco claras V35. Definição das regras má executadas V21. Responsabilidades ou obrigações contratuais externas à nuvem

Tabela 7.2 - Riscos políticos e organizacionais - Perda de governança (R2) (cont.)

Adaptado de [ENISA]

Vulnerabilidades	V23. Cláusulas do SLA com promessas conflitantes para diferentes partes interessadas V25. Auditoria ou certificação não estão disponíveis para os clientes V22. Aplicações entre nuvens, criando dependência obscura V13. Falta de tecnologias e soluções padrão V29. Armazenamento de dados em várias jurisdições e falta de transparência V14. Nenhum acordo sobre a propriedade do código-fonte (Paas e Saas) V16. Sem controle sobre o processo de avaliação de vulnerabilidade V26. Esquemas de certificação não adaptados às infra-estruturas de nuvem V30. Falta de informação sobre as jurisdições V31. Falta de integridade e transparência nos termos de uso V44. Propriedade dos ativos não é clara
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A3. Experiência e lealdade do funcionário A5. Dados pessoais sensíveis A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.3 - Riscos políticos e organizacionais - Desafios relacionados à conformidade (R3)

Adaptado de [ENISA]

Probabilidade	Muito Alta
Impacto	Alto
Vulnerabilidades	V13. Falta de tecnologias e soluções padrão V25. Falta de certificações e auditoria V26. Esquemas de certificação não adaptados às infra-estruturas de nuvem V29. Armazenamento de dados em múltiplas jurisdições e falta de transparência V30. Falta de informação sobre as jurisdições V31. Falta de integridade e transparência nos termos de uso
Recursos afetados	A20. Certificações
Nível do Risco	Alto

Tabela 7.4 - Riscos políticos e organizacionais - Perda de reputação devido a atividades de outros clientes (R4)

Adaptado de [ENISA]

Probabilidade	Baixa
Impacto	Alto
Vulnerabilidades	V5. Vulnerabilidades do *Hypervisor* V6. Falta de isolamento de recursos V7. Falta de isolamento à reputação
Recursos afetados	A1. Reputação da empresa A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.5 - Riscos políticos e organizacionais - Encerramento das atividades ou falhas por parte do provedor (R5)

Adaptado de [ENISA]

Probabilidade	N/A
Impacto	Muito Alto
Vulnerabilidades	V31. Falta de integridade e transparência nos termos de uso V46. Má escolha de provedor V47. Falta de redundância do fornecedor
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A3. Experiência e lealdade do funcionário A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Médio

Tabela 7.6 - Riscos políticos e organizacionais - Negociação entre fornecedores (R6)

Adaptado de [ENISA]

Probabilidade	N/A
Impacto	Médio
Vulnerabilidades	V31. Falta de integridade e transparência nos termos de uso
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A3. Experiência e lealdade do funcionário A4. Propriedade intelectual A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A8. Dados de alto risco A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Médio

Tabela 7.7 - Riscos políticos e organizacionais - Falha da cadeia de fornecimento (R7)

Adaptado de [ENISA]

Probabilidade	Baixa
Impacto	Médio
Vulnerabilidades	V22. Aplicações entre nuvens, criando dependência obscura V31. Falta de integridade e transparência nos termos de uso V46. Má escolha de provedor V47. Falta de redundância do fornecedor
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Médio

Tabela 7.8 - Riscos Técnicos - Falta de recursos (R8)

Adaptado de [ENISA]

Probabilidade	A. Impossibilidade de fornecer capacidade adicional: Média
	B. Impossibilidade de fornecer capacidade contratada: Baixa
Impacto	A. Impossibilidade de fornecer capacidade adicional: Baixo/Médio (e.g., Natal).
	B. Impossibilidade de fornecer capacidade contratada: Alto
Vulnerabilidades	V15. Modelagem imprecisa de uso do recurso V27. Provisionamento de recursos e investimento em infra-estrutura inadequados V28. Ausência de políticas para a limitação de recurso V47. Falta de redundância do fornecedor
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A10. Prestação de serviços A11. Controle de acesso, autenticação e autorização
Nível do Risco	Médio

Tabela 7.9 - Riscos Técnicos - Isolamento a falhas (R9)

Adaptado de [ENISA]

Probabilidade	Baixa (Nuvem privada) Média (Nuvem pública)
Impacto	Muito Alto
Vulnerabilidades	V5. Vulnerabilidades do Hypervisor V6. Falta de isolamento de recursos V7. Falta de isolamento à reputação V17. Possibilidade de a rede interna (nuvem) ser sondada V18. Possibilidade de inquilinos da mesma nuvem visualizarem recursos compartilhados
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.10 - Riscos Técnicos - Funcionários maliciosos por parte do provedor (R10)

Adaptado de [ENISA]

Probabilidade	Média
Impacto	Muito alto
Vulnerabilidades	V1. Vulnerabilidades nas contas de usuários, autenticação e autorização V10. Impossibilidade de processar dados de forma criptografada V34. Papéis e responsabilidades pouco claras V35. Definição das regras má executadas V36. Princípio da "informação sigilosa" não aplicado V37. Procedimentos de segurança física inadequados V39. Vulnerabilidades no Sistema Operacional V48. Aplicações vulneráveis ou má gestão de atualizações

Tabela 7.10 - Riscos Técnicos - Funcionários maliciosos por parte do provedor (R10) (cont.)

Adaptado de [ENISA]

Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A3. Experiência e lealdade do funcionário A4. Propriedade intelectual A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A8. Dados de alto risco A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.11 - Riscos Técnicos - Interfaces de administração vulneráveis (R11)

Adaptado de [ENISA]

Probabilidade	Média
Impacto	Muito alto
Vulnerabilidades	V1. Vulnerabilidades nas contas de usuários, autenticação e autorização V4. Interfaces remotas de gerenciamento V38. Configuração inadequada ou incorreta V39. Vulnerabilidades no Sistema Operacional V48. Aplicações vulneráveis ou má gestão de atualizações
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços A14. Interface de gerenciamento de serviços da nuvem
Nível do Risco	Médio

Tabela 7.12 - Riscos Técnicos - Interceptação de dados em trânsito (R12)

Adaptado de [ENISA]

Probabilidade	Média
Impacto	Alto
Vulnerabilidades	V1. Vulnerabilidades nas contas de usuários, autenticação e autorização V8. Vulnerabilidades na criptografia de dados em trânsito V9. Falta de criptografia de arquivos e dados em trânsito V17. Possibilidade de a rede interna (nuvem) ser sondada V18. Possibilidade de inquilinos da mesma nuvem visualizarem recursos compartilhados V31. Falta de integridade e transparência nos termos de uso
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A4. Propriedade intelectual A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A8. Dados de alto risco A23. Backup ou arquivamento de dados
Nível do Risco	Médio

Tabela 7.13 - Riscos Técnicos - Vazamento de dados no upload/download (R13)

Adaptado de [ENISA]

Probabilidade	Média
Impacto	Alto
Vulnerabilidades	V1. Vulnerabilidades nas contas de usuários, autenticação e autorização V8. Vulnerabilidades na criptografia de dados em trânsito V10.Impossibilidade de processar dados de forma criptografada V17. Possibilidade de a rede interna (nuvem) ser sondada V18. Possibilidade de inquilinos da mesma nuvem visualizarem recursos compartilhados V48. Aplicações vulneráveis ou má gestão de atualizações

Tabela 7.13 - Riscos Técnicos - Vazamento de dados no upload/download (R13) (cont.)

Adaptado de [ENISA]

Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A3. Experiência e lealdade do funcionário A4. Propriedade intelectual A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A8. Dados de alto risco A12. Credenciais A13. Diretório do usuário (dados) A14. Interface de gerenciamento de serviços da nuvem
Nível do Risco	Médio

Tabela 7.14 - Riscos Técnicos - Eliminação de dados insegura ou ineficiente (R14)

Adaptado de [ENISA]

Probabilidade	Média
Impacto	Muito alto
Vulnerabilidades	V20. Limpeza de dados confidenciais
Recursos afetados	A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A12. Credenciais
Nível do Risco	Médio

Tabela 7.15 - Riscos Técnicos - Distributed Denial of Service (DDoS) (R15)

Adaptado de [ENISA]

Probabilidade	Cliente: Médio Provedor: Baixo
Impacto	Cliente: Alto Provedor: Muito alto

Tabela 7.15 - Riscos Técnicos - Distributed Denial of Service (DDoS) (R15) (cont.)

Adaptado de [ENISA]

Vulnerabilidades	V38. Configuração inadequada ou incorreta V39. Vulnerabilidades no Sistema Operacional V53. Recursos de filtragem inadequados ou mal configurados
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços A14. Interface de gerenciamento de serviços da nuvem A16. Rede (ligações, etc)
Nível do Risco	Médio

Tabela 7.16 - Riscos Técnicos - Economic Denial of Service (EDoS) (R16)

Adaptado de [ENISA]

Probabilidade	Baixa
Impacto	Alto
Vulnerabilidades	V22. Aplicações entre nuvens, criando dependência obscura V31. Falta de integridade e transparência nos termos de uso V46. Má escolha de provedor V47. Falta de redundância do fornecedor
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Médio

Tabela 7.17 - Riscos Técnicos - Perda da chave de criptografia (R17)

Adaptado de [ENISA]

Probabilidade	Baixa
Impacto	Alto
Vulnerabilidades	V11. Procedimentos para gerenciamento de chave deficiente V12. Geração de chaves: baixa entropia para a geração de números aleatórios

Tabela 7.17 - Riscos Técnicos - Perda da chave de criptografia (R17) (cont.)

Adaptado de [ENISA]

Recursos afetados	A4. Propriedade intelectual A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A8. Dados de alto risco A12. Credenciais
Nível do Risco	Médio

Tabela 7.18 - Riscos Técnicos - Testes maliciosos de varredura ou penetração (R18)

Adaptado de [ENISA]

Probabilidade	Média
Impacto	Médio
Vulnerabilidades	V17. Possibilidade de a rede interna (nuvem) ser sondada V18. Possibilidade de inquilinos da mesma nuvem visualizarem recursos compartilhados
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Médio

Tabela 7.19 - Riscos Técnicos - Plataformas vulneráveis (R19)

Adaptado de [ENISA]

Probabilidade	Baixa
Impacto	Muito alto
Vulnerabilidades	V5. Vulnerabilidades do Hypervisor V6. Falta de isolamento de recursos

Tabela 7.19 - Riscos Técnicos - Plataformas vulneráveis (R19) (cont.)

Adaptado de [ENISA]

Recursos afetados	A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A8. Dados de alto risco A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Médio

Tabela 7.20 - Riscos Técnicos - Conflitos entre os processos de segurança do cliente e da nuvem (R20)

Adaptado de [ENISA]

Probabilidade	Baixa
Impacto	Médio
Vulnerabilidades	V23. Cláusulas do SLA com promessas conflitantes para diferentes partes interessadas V31. Falta de integridade e transparência nos termos de uso V34. Papéis e responsabilidades pouco claras
Recursos afetados	A4. Propriedade intelectual A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico
Nível do Risco	Médio

Tabela 7.21- Riscos Legais - Intimação e confisco de hardware (R21)

Adaptado de [ENISA]

Probabilidade	Alta
Impacto	Médio
Vulnerabilidades	V6. Falta de isolamento de recursos V29. Armazenamento de dados em várias jurisdições e falta de transparência V30. Falta de informação sobre as jurisdições

Tabela 7.21- Riscos Legais - Intimação e confisco de hardware (R21) (cont.)

Adaptado de [ENISA]

Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.22 - Riscos Legais - Riscos de mudanças de jurisdição (R22)

Adaptado de [ENISA]

Probabilidade	Muito alta
Impacto	Alto
Vulnerabilidades	V29. Armazenamento de dados em várias jurisdições e falta de transparência V30. Falta de informação sobre as jurisdições
Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.23 - Riscos Legais - Riscos de proteção de dados (R23)

Adaptado de [ENISA]

Probabilidade	Alta
Impacto	Alto
Vulnerabilidades	V29. Armazenamento de dados em várias jurisdições e falta de transparência V30. Falta de informação sobre as jurisdições

Tabela 7.23 - Riscos Legais - Riscos de proteção de dados (R23) (cont.)

Adaptado de [ENISA]

Recursos afetados	A1. Reputação da empresa A2. Confiança do cliente A5. Dados pessoais importantes A6. Dados pessoais A7. Dados pessoais - Crítico A9. Prestação de serviços - serviços em tempo real A10. Prestação de serviços
Nível do Risco	Alto

Tabela 7.24 - Riscos Legais - Riscos de licenciamento (R24)

Adaptado de [ENISA]

Probabilidade	Média
Impacto	Médio
Vulnerabilidades	V31. Falta de integridade e transparência nos termos de uso
Recursos afetados	A1. Reputação da empresa A9. Prestação de serviços - serviços em tempo real A20. Certificações
Nível do Risco	Médio