CAROLINA BARBOSA RIBEIRO

PROCESSO DE GESTÃO DE RISCO PARA O CONTROLE DA SEGURANÇA NA COMPUTAÇÃO EM NUVEM

Monografia apresentada ao PECE – Programa de Educação Continuada da Universidade de São Paulo, como parte dos requisitos para obtenção do título de Especialista em Tecnologia da Informação.

Orientador: Prof. Dr. Stephan Kovach.

São Paulo

2012

CAROLINA BARBOSA RIBEIRO

PROCESSO DE GESTÃO DE RISCO PARA O CONTROLE DA SEGURANÇA NA COMPUTAÇÃO EM NUVEM

São Paulo
2012

FICHA CATALOGRÁFICA

Ribeiro, Carolina Barbosa
Processo de gestão de risco para o controle da segurança na computação em nuvem / C.B. Ribeiro. -- São Paulo, 2013.
55 p.

Monografia (MBA em Tecnologia da Informação) - Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1.Informação (Segurança) 2.Computação em nuvem 3.Gestão de risco I.Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II.t.

CAROLINA BARBOSA RIBEIRO

PROCESSO DE GESTÃO DE RISCO PARA O CONTROLE DA SEGURANÇA NA COMPUTAÇÃO EM NUVEM

Monografia apresentada ao PECE – Programa de Educação Continuada da Universidade de São Paulo, como parte dos requisitos para obtenção do título de Especialista em Tecnologia da Informação.

Orientador: Prof. Dr. Stephan Kovach.

Aprovação em:

São Paulo

2012

Dedico esta monografia aos meus pais, Luiz e Elizabete, pelo apoio, dedicação, amor e carinho cedidos a mim. E agradecimentos ao professor Stephan Kovach pela orientação e ajuda para a criação deste trabalho.

RESUMO

A computação na nuvem é uma tecnologia emergente em rápida evolução que promete a redução dos custos em TI, obrigando as empresas permanecerem atualizados com os processos de TI e aumentar a inovação tecnológica.

Como qualquer nova tecnologia, a computação na nuvem cria novos riscos e novas oportunidades. Em alguns casos, migrar para nuvem prevê uma oportunidade de reestruturar aplicações antigas (os conhecidos legados) e infraestrutura para adequar ou exceder os requisitos de segurança da informação. Às vezes o risco de mover dados confidenciais e aplicações para uma infraestrutura emergente pode estar além da tolerância aceitável.

Este trabalho pretende apresentar uma adaptação da norma ISO/IEC 27005 para o processo de gestão de risco de segurança da informação aplicado aos modelos de serviço e implementação de computação em nuvem, reconhecendo os cenários de riscos inerentes a cada um desses modelos, visando atender os requisitos de segurança da informação, segundo a norma ISO/IEC 18028, exigidos pelos ativos de informação passíveis de transferência para a nuvem.

ABSTRACT

Cloud computing is an emerging technology that evolves rapidly, reducing IT costs, forcing companies to keep up to date with IT processes and increase technological innovation.

As any new technology, cloud computing creates new risks and new opportunities. In some cases, migrating to cloud provides an opportunity to restructure legacy applications and infrastructure to match or exceed the requirements of information security. Sometimes the risk of confidential data and applications moving to an emerging infrastructure may be beyond tolerance.

This work aims to provide ways to identify analyze and mitigate information security risks to the assets eligible for transferring to the cloud, through the process of risk management adapted from ISO/IEC 27005.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

IEC - International Engineering Consortium

ISO – International Standards Organization

NIST – National Institute of Standards and Technology

CSA - Cloud Security Alliance

SAAS – Software as a Service

PAAS – Plataform as a Service

IAAS – Infrastructure as a Service

SGSI - Sistema de gerenciamento de segurança da informação

SLA - Service Level Agreement

SUMÁRIO

1. INTRODUÇÃO

1.1. Considerações iniciais

A computação na nuvem é um novo conceito tecnológico que muda a maneira como a solução de arquitetura de TI é apresentada, avançando temas como virtualização de armazenamento de dados, infraestrutura e de software como serviço.
Entretanto, essa tecnologia não é apenas uma inovação e sim, uma solução estratégica de negócio para as empresas.

No entanto, mesmo sendo uma solução promissora no mercado, a questão de segurança na computação na nuvem é de fundamental importância e um dos principais questionamentos inclui a garantia de confidencialidade e integridade dos dados, as políticas de segurança, a dinâmica de serviços e a confiança entre as entidades. (ZHOU *et al.*,2010).

1.2. Objetivo

O objetivo desse trabalho é apresentar uma adaptação da norma ISO/IEC 27005 (ISO/IEC 27005:2008) para o processo de gestão de risco de segurança da informação aplicado aos modelos de serviço e implementação de computação em nuvem, reconhecendo os cenários de riscos inerentes a cada um desses modelos, visando atender os requisitos de segurança da informação, segundo a ISO/IEC 18028 (ISO/IEC 18028:2006), exigidos pelos ativos de informação passíveis de transferência para a nuvem.

1.3. Motivação

Com o crescimento da necessidade de processar diferentes volumes de informações, as maiores oportunidades de atender essa necessidade estão relacionadas com a computação em nuvem. Porém, a grande maioria das empresas ainda desconhece como a segurança é tratada nesta tecnologia e ainda imaginam, de forma equivocada, que provedores de serviços externos tenham menos condições de proteger as informações do que os recursos internos da própria

empresa. Deste modo, a adoção de computação na nuvem depende da clarificação de como este aspecto podem ser tratado.

Este trabalho é baseado nas exigências da governança e da gestão de TI no controle da segurança na computação em nuvem. Este estudo se baseia nos padrões corporativos de segurança como a ISO/IEC 18028, que descreve os requisitos de segurança da informação, e a ISO/IEC 27005 aplicados no controle e gestão de risco de segurança da informação nos modelos de implementação e serviços oferecidos pelos provedores de computação na nuvem.

1.4. Estrutura do trabalho

O trabalho está organizado como segue:

O capítulo dois explica os temas teóricos que destacam de forma sucinta as características e os modelos de serviço e de implementação na nuvem e as respectivas aplicabilidades e pontos de atenção, e a norma ISO/IEC 27005 que explica como é o processo de gestão de risco de segurança da informação.

O capítulo três apresenta aos requisitos de segurança da informação que devem ser considerados e avaliados no processo de gestão de risco de segurança da informação na computação em nuvem.

No capítulo quatro, é apresentado os cenários de riscos referentes aos modelos de serviço e de implementação de computação na nuvem, e em seguida, o processo de gestão de risco adaptado da norma ISO 27005.

O trabalho é finalizado com as considerações finais no capítulo cinco.

2. FUNDAMENTAÇÃO TEÓRICA

2.1. Modelos de Computação na Nuvem

A computação na nuvem é um termo que descreve um ambiente de computação baseado em uma imensa rede de servidores, sejam estes virtuais ou físicos, este ambiente é conhecido como *Data Center.*

Uma definição simples pode, então, ser "um conjunto de recursos com capacidade flexível, escalável e distribuído de processamento, armazenamento, conectividade, plataformas e aplicações, providos como serviço disponibilizado na Internet" (TAURION, 2009).

De acordo com a NIST (NIST, 2011), a Computação em Nuvem é um modelo que permite acesso à rede sob demanda de maneira onipresente e conveniente, a um *pool* compartilhado de recursos de computação configuráveis, que podem ser provisionados e liberados de forma rápida e com mínimo esforço de gerenciamento. Na prática, a Computação em Nuvem seria a transformação dos sistemas computacionais físicos de hoje em uma base virtual.

O modelo de nuvem é composto de cinco características essenciais, três modelos de serviços e quatro modelos de implementação, e serão detalhados no decorrer deste capítulo.

2.2. Modelos de Serviço na Nuvem

No modelo de serviço na nuvem, a aplicação, a plataforma e a infraestrutura, são fornecidas como serviços dimensionados, e de acordo com o NIST (NIST, 2011), existem atualmente três modelos básicos de computação em nuvem, conforme a figura 1 os modelos presentes são:

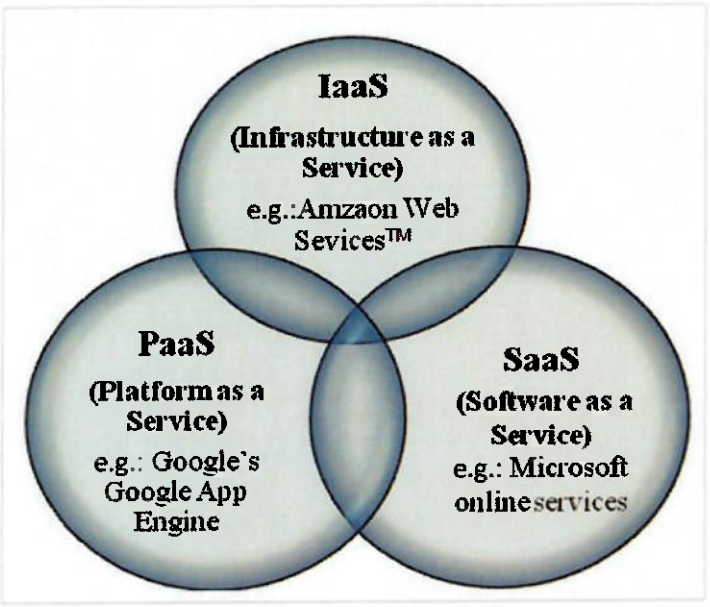

Figura 1 - Modelos de serviços presentes na computação na nuvem. [Fonte: WEN-HSI, 2012]

2.3. Modelo *Software-as-a-Service*

O modelo *SaaS* é a oferta de software através de um provedor de serviços terceirizado. Neste modelo, o software é disponibilizado através de uma conexão de Internet, onde o cliente aluga a solução total do software remotamente.

Alguns exemplos da aplicabilidade do modelo *SaaS* são: ferramentas de Colaboração (ex: *DropBox*), serviços de CRM (ex: *Oracle OnDemand*, *Saleforce.com*), Contabilidade (ex: *Aria Systems* e *OpSource*), Financeiro (ex: *Xero* e *Concur*), Vendas (ex: *Xactly* e *LucidEra*), Recursos Humanos (ex: *Taleo*, *Workday*, *iCIMS*), Backup & Reparação (ex: *JungleDisk*, *OpenRSM* e *Mozy*), Gerenciamento de Conteúdo e Documentos (ex: *SpringCM*, *NetDocuments*), Serviços de Web Mail (ex: *Gmail*) ou qualquer conteúdo Web.

A lista abaixo mostra os pontos de atenção do modelo:

- Segurança - Ainda existem dúvidas (por parte dos consumidores) sobre a segurança dos dados (localização e segregação), e a compreensão insuficiente dos recursos do *SaaS*.
- Incompatibilidade de negócio - o risco de negócio do cliente não atender aos recursos disponíveis do serviço *SaaS*.

- Dependência dos recursos e tecnologia do provedor.

2.3.1. Modelo *Plataforma-as-a-Service*

O modelo *PaaS* é definido como sendo a plataforma virtual pré-carregada com sistemas operacionais, para criar e operar aplicações, incluindo ferramentas de desenvolvimento, administração e gerenciamento.

A aplicabilidade do modelo *PaaS* reduz os esforços necessários de configuração e mantem essa camada restrita ao desenvolvimento e a implantação de aplicações.

Alguns exemplos da aplicabilidade do modelo *PaaS* são: ferramentas de uso geral para prover serviços web (ex: *Force.com*, *Google App Engine* e *MS Azure Services Plataform*), ferramentas de *Business Intelligence* (ex: *Vertica*, *Parorama*, *Aster DB* e *Cloud9 Analytics*), ferramentas para Integração de sistemas para prover a computação distribuída (ex: *Amazon SQS*, *MuleSource Mule On Demand* e *Microsoft BizTalk Services*), ferramenta de desenvolvimento e testes de aplicações (ex: *Collabnet*, *Dynamsoft*, *Keynote Systems* e *Mercury*), e de Banco de Dados (ex: *Google BigTable*, *Amazon SimpleDB*, *Microsoft SDS*).

Na lista a seguir são mostrados os pontos de atenção do modelo *PaaS*:

- Dependência do provedor – As aplicações desenvolvidas de acordo com os recursos fornecidos de um provedor de *PaaS* pode não ser compatível para um outro provedor.
- Complexidade de Integração – maior complexidade de comunicação entre sistemas internos do consumidor com os sistemas na nuvem, dificultando a utilização dos dados na nuvem em conjunto com os dados locais.

2.3.2. Modelo *Infraestructure-as-a-Service*

O modelo *IaaS* oferece toda a parte de hardware virtual (servidores, rede, armazenamento etc), na qual o cliente deve implantar e executar toda a sua camada de aplicações e base de dados, websites e sistemas de TI.

Alguns exemplos da aplicabilidade do modelo *IaaS* são: serviço de armazenamento (ex: *Amazon S3*, *Amazon EBS*, *CTERA Portal*), recursos computacionais (ex: *Amazon EC2*, *AppNexus*, *Elastra*, *Flexiscale*, *GridLayer*, *Elastichosts*) e serviços de gerenciamento (ex: *RightScale*, *CohesiveFT*, *CloudFoundry*, *enStratus*)

Na lista abaixo são mostrados os pontos de atenção do modelo *IaaS*:

- Segurança - a preocupação dos usuários de perder o controle total de seus dados. Muitos provedores de *IaaS* oferecem um ambiente em nuvem privada como uma tentativa para combater este argumento.
- *Aspectos Legais* - Desconhecimento do usuário sobre a localização física dos dados, e se o local armazenado reside em região geográfica legal e de acordo com as conformidades (leis e regulamentos) para a organização.

2.4. Modelos de Implementação na Nuvem

Segundo o *NIST*, a decisão sobre um modelo de implementação depende das necessidades, restrições e dos requisitos das aplicações que serão implementadas. A figura 2 apresenta a divisão representando os diferentes tipos de implementação de nuvem: (NIST, 2011).

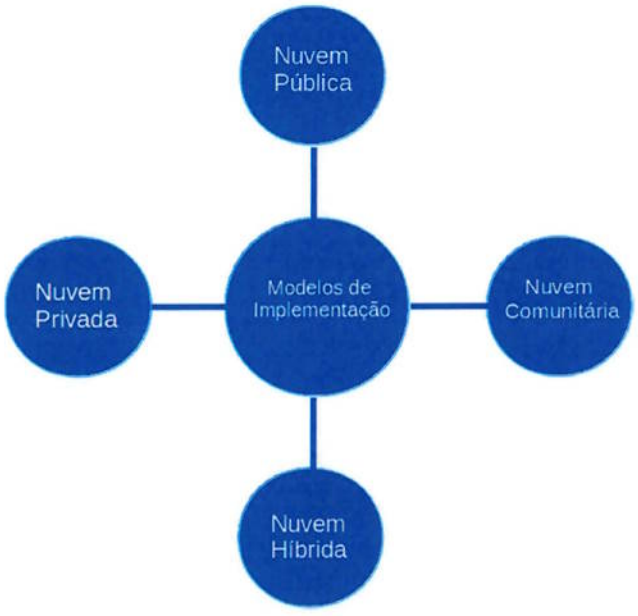

Figura 2 - Modelos de implementação de computação na nuvem. [Fonte: WEN-HSI, 2012]

2.4.1. Modelo de Implementação de Nuvem Pública

O modelo de nuvem pública é provisionado para uso aberto para o público em geral. Pode ser mantida, gerenciada e operada por organizações, por universidades, pelo governo ou empresa, ou através de uma combinação entre diferentes organizações.

Este modelo é hospedado dentro das instalações (*Data Centers*) do provedor de serviços (terceiro).

A lista abaixo mostra os pontos de atenção aplicados ao modelo de implementação de nuvem pública:

- Controle reduzido: o cliente reduz o controle de seu sistema de TI e da localização dos dados, e é completamente dependente do fornecedor de serviços;
- Segurança dos dados: Uma vez que os recursos são compartilhados entre diferentes entidades, há riscos elevados de violações de acesso de confidencialidade;
- Responsabilidades de Segurança: considerar a variação de responsabilidades compartilhada entre o fornecedor e o usuário;
- Garantir a criptografia dos dados: para a confidencialidade da informação.

2.4.2. Modelo de Implementação de Nuvem Privada

O modelo de nuvem privada é provisionado para uso exclusivo de uma única organização, onde pode ser hospedada, gerenciada e operada pelo consumidor da nuvem, por um provedor de serviços (terceiro) ou através de uma combinação deles. (NIST, 2011).

A lista abaixo apresenta os pontos de atenção deste modelo:

Atualização - O modelo pode ficar diretamente atrelado aos processos corporativos, tornando-se engessado em termos de automação de tarefas como atualizações e manutenção.

Maior investimento com gerenciamento interno - Embora o modelo provê um menor risco e algumas facilidades de negócio, exige um investimento no gerenciamento interno, o que diminui a economia de recursos.

2.4.3. Modelo de Implementação de Nuvem Comunitária

O modelo de nuvem comunitária é provisionado para uso exclusivo por uma comunidade específica de consumidores (organizações) que prove de preocupações em comum (missão, requisitos de segurança, políticas e requisitos legais em comum).

Pode ser hospedada, gerenciada e operada por uma ou mais organizações desta comunidade, ou por um provedor de serviços (terceiro), ou pela combinação de organizações e provedores.

Os pontos de atenção do modelo de implementação de nuvem comunitária são os mesmos do modelo de implementação de nuvem privada.

2.4.3.1 Modelo de Implementação de Nuvem Híbrida

O modelo de nuvem híbrida é provisionada por duas ou mais infraestruturas de nuvens distintas (comunidade, particular ou pública) unidas por tecnologia proprietária ou padronizadas, permitindo a portabilidade de aplicações ou dados.

A lista abaixo mostra os pontos de atenção do modelo de implementação de nuvem híbrida:

- Extensão do perímetro: A nuvem híbrida tem maior extensão de TI além dos limites organizacionais, e abre-se uma maior probabilidade de ataques principalmente na nuvem pública a qual fica sob controle do provedor;
- Gerenciamento de identidade e acesso: Importância de estender a identidade corporativa e o gerenciamento de acesso para as nuvens públicas. Isso abre as preocupações sobre como esta abordagem irá afetar a identidade da empresa e seu impacto na segurança da organização;

- Ferramentas de gestão: O cliente deve considerar as implicações de segurança do uso de ferramentas de gestão. A ferramenta de gestão deve ser capaz de lidar com a identidade e garantir a segurança de maneira uniforme no modelo de nuvem híbrida;

- Migração de dados: Com a facilidade do fluxo de dados entre os modelos, há preocupações de privacidade e integridade de dados, porque os controles de privacidade do modelo de nuvem pública variam significativamente do modelo privado;

- Políticas de segurança: Existem riscos associados com as políticas de segurança que medem o ambiente de nuvem híbrida, como problemas com a forma como as chaves de criptografia são gerenciadas em uma nuvem pública em comparação ao ambiente de nuvem privada pura;

2.5. Características da Computação na Nuvem

As características atendem a todos os tipos de modelo de computação na nuvem. São:

- **Autoatendimento sob demanda (*On-demand self-service*):** Um usuário pode, unilateralmente, provisionar recursos de computação com processamento de servidores ou armazenamento em rede, conforme necessário, sem necessidade de interação com o provedor de serviços. (NIST, 2011).

- **Amplo acesso à rede:** Recursos estão disponíveis através da rede e podem ser acessados por meio de mecanismos que possibilitem o padrão utilizado por plataformas heterogêneas (por exemplo, telefones celulares, tablets, notebooks e estações de trabalho). (NIST, 2011)

- ***Pooling* de recursos:** Os recursos do provedor de computação são agrupados para atender vários usuários através de um modelo *multi-tenant* (uma instância de software que atende múltiplos clientes), com diferentes recursos físicos e virtuais atribuídos dinamicamente, de acordo com a demanda do consumidor. (NIST, 2011).

- **Rápida elasticidade**: Ampla capacidade de provisionamento de forma escalável e proporcional (crescimento e decrescimento) de acordo com a demanda. Para o consumidor, as capacidades disponíveis para provisionamento frequentemente parecem ser ilimitadas e podem ser apropriadas em qualquer quantidade a qualquer momento. (NIST, 2011).

- **Serviço mensurado:** Sistemas na nuvem automaticamente controlam e otimizam o uso dos recursos, aproveitando a capacidade apropriada para o tipo de serviço (por exemplo, processamento, armazenamento, largura de banda e contas de usuários ativos). O uso de recursos pode ser monitorado, controlado e reportado, oferecendo transparência para o provedor e para o consumidor do serviço utilizado. (NIST, 2011).

Geralmente o cliente não tem o controle ou o conhecimento sobre a localização exata dos recursos disponibilizados, mas pode ser capaz de especificar o local em um nível maior de abstração (por exemplo, estado, país, ou *datacenter*).

Nos dias de hoje, as organizações estão buscando a Computação na Nuvem visando expandir sua infraestrutura, porém a maioria não pode correr riscos de comprometer a segurança de aplicativos e dados.

Na decisão e escolha pelo tipo de serviço e implementação, gerentes de negócios precisam avaliar a segurança considerando o ponto de vista arquitetônico da empresa, levando-se em conta as divergências de segurança da informação para cada modelo de implementação e de serviço. Essas divergências serão discutidas no capítulo quatro, onde serão destacados os principais riscos para cada modelo.

2.6. Principais Provedores de Computação na Nuvem

Entre algumas organizações que provêm modelos de computação na nuvem destacam-se a Amazon, Google, IBM e a Microsoft.

A Amazon com a chamada *Amazon Web Services* (*AWS*) fornece ofertas de serviço na nuvem como o *EC2* (*Elastic Computing Cloud*), para alugar máquinas virtuais, onde o usuário pode alugar CPUs, o *S3* como serviço de armazenamento (storage) na nuvem, o *SimpleDB* como serviço de *Database-as-a-Service* e o *SQS* (*Simple*

Queue Service) para serviços de mensageria. A ideia é que os usuários possam operar seu negócio pagando apenas pelo uso de espaço em disco.

O Google oferece o *Google AppEngine*, um ambiente que permite ao desenvolvedor criar aplicações sem a necessidade de servidor e software específicos. Todo o trabalho é feito na nuvem e a aplicação é projetada para rodar exclusivamente no Google. O *AppEngine* é tecnicamente competidor do *EC2* da Amazon, mas oferece uma proposta diferente. O *EC2* permite mais flexibilidade e controle por parte do usuário, enquanto o *AppEngine* oferece mais facilidade de uso, onde o usuário escreve o código, carrega sua aplicação e o Google se responsabiliza por gerenciar outros recursos computacionais (como Hardware, Rede, Servidor de Aplicação, Integração Contínua, Controle de Versão, Deployment, Banco de Dados, etc).

A IBM conta com os serviços da *Blue Cloud* onde através do portal web, o usuário pode especificar a plataforma de hardware, o tipo de processador, capacidade de memória e armazenamento, o sistema operacional, e utilizar os serviços da *IBMTivoli* e a *LotusLive*.

O objetivo da IBM é levar o modelo de computação na nuvem para os data centers, desenhando modelos híbridos, no qual parte da TI do cliente consumidor pode estar dentro de casa, mas operando de forma automática e eficiente (modelo de nuvem) e parte operando em nuvens públicas, externas, deixando a cargo destas aplicações que não sejam críticas para o negócio.

Implantar uma nuvem interna é um caminho para grandes empresas, e a IBM iniciou em direção à computação sob demanda, com o anúncio da sua estratégia *e-business on demand*.

A Microsoft lançou a tecnologia chamada *WindowsAzure*, sendo um conjunto de serviços de *Plataform-as-a-Service* chamada *Azure Services Plataform*, focada nos desenvolvedores.

Há uma grande diferença nas propostas oferecidas pela Amazon, Google e Microsoft. A proposta da *EC2* é similar à de um servidor físico, com os usuários controlando toda a pilha de software, não havendo limite quanto ao tipo de aplicação que pode ser executada. O Google *AppEngine*, por sua vez, é orientado a

aplicações web, limitado a linguagens e ambientes específicos. O *Azure* se situa em um ponto intermediário, as aplicações são escritas na linguagem *.Net* e compiladas no ambiente próprio. O desenvolvedor escolhe a linguagem, mas não escolhe o ambiente computacional, restrito ao *Windows*.

2.7. Norma ISO/IEC 27000

A série da norma ISO/IEC 27000 foi reservada especificamente pela ISO dedicada as questões de segurança da informação. Ela se alinha com uma série de outros tópicos, incluindo a ISO 9000 (gestão da qualidade) e a ISO 14000 (gestão ambiental). A série da norma ISO/IEC 27000 é constituída por um conjunto de normas operacionais conforme apresentadas na tabela 1.

Tabela 1 - Principais normas operacionais da série ISO/IEC 27000.

ISO/IEC 27001. Especificação para a gestão de segurança de sistemas de informação. A Norma substituiu a conhecida norma BS7799-2.	**ISO/IEC 27002** Norma para as práticas na gestão da segurança da informação, originada da norma ISO 17799.
ISO/IEC 27003 Novo padrão para oferecer orientações para a aplicação de um SGSI (Sistema de gerenciamento de segurança da informação).	**ISO/IEC 27004** Esta norma abrange informações de segurança na medição de sistemas de gestão e métricas, incluindo os controles alinhados a ISO 27002.
ISO/IEC27005 Norma para a gestão de riscos de segurança da informação. Visa a facilitar a implementação da segurança da informação tendo como base a gestão de riscos.	**ISO/IEC 27006** A norma fornece diretrizes para o credenciamento de organizações que oferecem certificação SGSI.

A adoção dessas normas deve ser uma decisão estratégica, onde o desenho e a implementação de um Sistema de Gestão de Segurança são influenciados pelas necessidades, objetivos, requisitos de segurança, processo empregado e pelo tamanho e estrutura da organização. (IsecT, 2012).

No desenvolvimento deste trabalho, foi tomado como base de estudo as práticas e diretrizes de segurança da informação sugeridas pelas normas 27005.

2.7.1. Norma ISO/IEC 27005 – Gestão de Risco de Segurança da Informação

A norma ISO/IEC 27005 fornece as diretrizes para um processo genérico na Gestão de Riscos de Segurança da Informação de uma organização. A norma dá sustentação aos conceitos da norma ISO/IEC 27001(ISO/IEC 27001:2005), além de auxiliar na maneira de implementar e certificar os sistemas de gestão nas organizações.

O processo descrito pela norma é sincronizado com o ciclo de melhoria contínua PDCA *(Plan, Do, Check, Act)*, o qual é aplicado para estruturar todos os processos do SGSI (Sistema de Gerenciamento de Segurança da Informação), descrito da norma a ISO/IEC 27001.

A figura 3 mostra o ciclo de implementação PDCA, onde os requisitos de segurança são a fonte de informações que alimenta este ciclo (input) e o processo de segurança da informação gerenciado é o resultado deste ciclo (output).

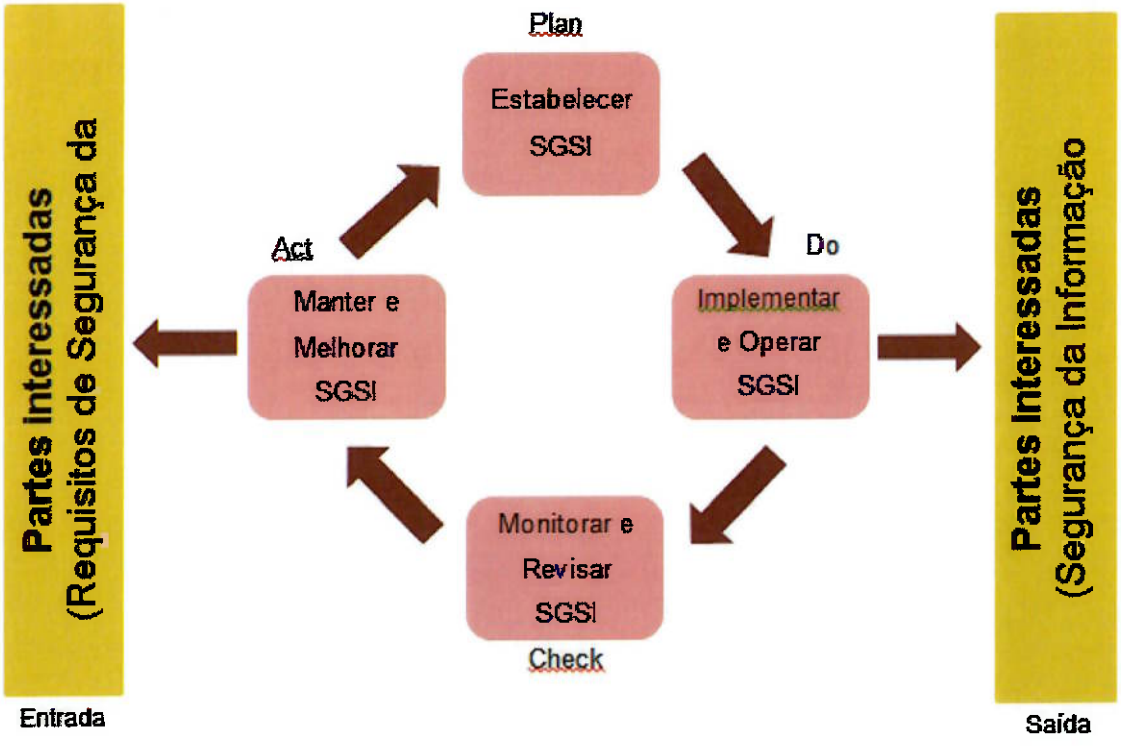

Figura 3 - Ciclo de implementação do PDCA. [Fonte: IsecT, 2012]

Este processo é a transformação de entradas em saídas que utilizam um conjunto de atividades inter-relacionadas em cada interação. A saída de um processo pode automaticamente dar início a um novo processo, isto é feito normalmente de forma planejada e controlada por todos os atores (por exemplo: gestores, analista e consultores).

A norma é aplicável a todos os tipos de organização, e não fornece ou recomenda uma metodologia específica. Ela pode ser adaptada conforme as necessidades da organização.

O processo de gestão de risco de segurança é consiste na criação de um contexto, na avaliação de risco, no tratamento de riscos, na aceitação e comunicação de risco, monitoramento de riscos e revisão do processo, conforme mostrado na figura 4:

Processo de Gestão de Risco

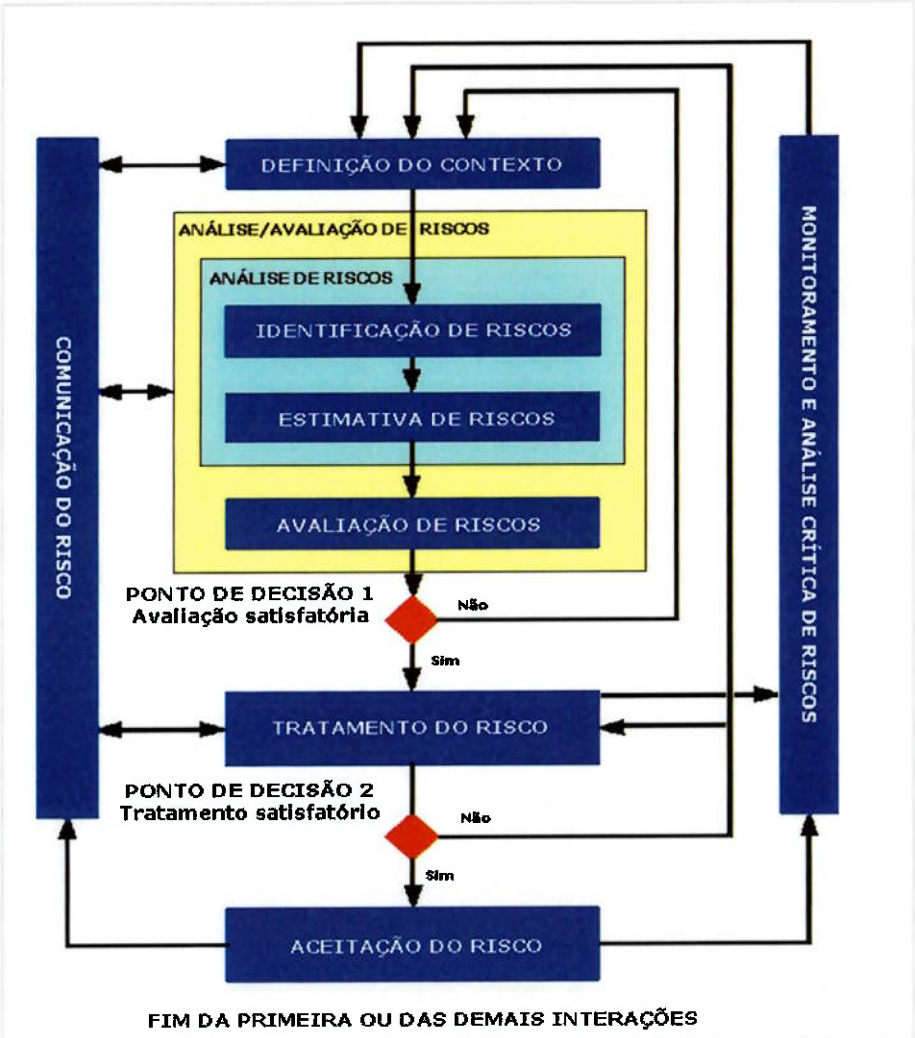

Figura 4 – Etapas do processo para a gestão de risco de segurança da informação. [Fonte: ISO/IEC 27005]

De acordo com a figura 4, o processo de gestão de risco é um processo iterativo. Uma abordagem iterativa para realizar a avaliação de risco pode aumentar o nível de detalhe da avaliação a cada iteração.

Inicialmente, o contexto é criado (o contexto é o tema que será aplicado no processo de gestão). Em seguida, uma avaliação de risco é realizada. Se as informações (por ex: critérios para avaliação, aceitação e de impacto do risco) são suficientes para determinar as ações necessárias para modificar os riscos a um nível aceitável, a tarefa está concluída e o tratamento de riscos, segue. Se as informações forem insuficientes, outra iteração de avaliação de risco com o contexto revisado será realizada.

A eficácia do tratamento do risco depende dos resultados da avaliação dos riscos. É possível que o tratamento de risco não conduza de imediato para um nível aceitável de risco, e deste modo é comum que outras iterações sejam feitas para avaliar os critérios de avaliação.

A atividade de aceitação do risco tem de garantir que os riscos identificados sejam expressamente aceitos pelos gestores da organização. Isto é importante em uma situação onde a implementação de controles é omitida ou adiada, por exemplo, devido ao custo.

Durante o processo de gerenciamento, é importante que os riscos e seu tratamento sejam comunicados aos envolvidos, e os resultados detalhados a cada atividade do processo de gestão de riscos de segurança da informação e dos pontos de decisão de risco devem ser documentados.

A norma ISO 27001 especifica que os controles implementados no âmbito, nos limites e no contexto dos SGSIs devem ser baseados no risco. As organizações devem usar o que melhor se adequa as suas circunstâncias, e são livres para escolher quaisquer controles de segurança da informação aplicáveis a situações particulares (IsecT, 2012).

3. REQUISITOS PARA A SEGURANÇA DA INFORMAÇÃO APLICADOS AO AMBIENTE NA NUVEM

Atualmente é cada vez mais frequente a necessidade das empresas assegurarem a confidencialidade, a integridade e a disponibilidade dos dados no momento que forem transmitidos, armazenados ou processados em um ambiente externo e controlado por terceiros na cadeia de serviços em nuvem.

Antes de abordar o assunto sobre gestão e controle de riscos de segurança na nuvem, é importante destacar e compreender os principais requisitos de segurança da informação, baseados na norma ISO/IEC 18028, que serão mostrados no decorrer deste capítulo.

3.1. Requisitos de Segurança

Segundo a norma ISO/IEC 18028, uma série de requisitos de segurança da informação é sugerida. Eles serão usados como guia também para a segurança na nuvem a fim de tornar-se uma solução de tecnologia eficaz e segura. Estes requisitos são definidos a seguir.

3.1.1. Autenticação (Identificação) e Autorização

A pergunta mais comum sobre o armazenamento compartilhado é se usuários não autorizados podem acessar a informação intencionalmente ou por engano.
Segunda a norma ISO/IEC 18028,

> a autenticação serve para confirmar as identidades ou outros atributos que autorizam entidades de comunicação. A autenticação garante a validade das identidades reivindicadas quando utilizando métodos de autorização ou de controle de acesso das entidades participantes na comunicação (por exemplo, pessoa, dispositivo, serviço ou aplicação) e fornece garantia de que a entidade não está tentando uma reprodução não autorizada de uma comunicação prévia.

Neste caso, os modelos de computação na nuvem devem oferecer flexibilidade ao consumidor para controlar os níveis de acesso, utilizando padrões que permitem acesso autenticado.

Dependendo do tipo do modelo (serviço e de implementação) de nuvem, os usuários que terão acesso a(s) entidade(s) devem ser estabelecidos em primeiro lugar e as prioridades complementares de acesso e permissões podem ser concedidas em conformidade. Este processo tem como alvo a verificação e validação dos usuários de nuvem individualmente, empregando nomes de usuários e senhas para proteger seus perfis em nuvem.

3.1.2. Confidencialidade

A confidencialidade significa manter os dados confidenciais do usuário em um ambiente na nuvem.

Segunda a norma ISO/IEC 18028,

> a confidencialidade protege os dados contra divulgação não autorizada. A criptografia é um método frequentemente utilizado para garantir a confidencialidade dos dados. Listas de controle de acesso e permissões de arquivos são métodos que ajudam a manter os dados confidenciais.

Atualmente, de acordo com (ZHOU *et al.* 2010), os serviços oferecidos no modelo de implementação de nuvem pública, as aplicações e sistemas são vulneráveis a mais ataques quando comparados com as aplicações hospedadas em *data centers* privados (modelo de implementação de nuvem privada).

Tradicionalmente, há duas abordagens básicas para alcançar a confidencialidade: o controle dos dados situados em vários bancos de dados distribuídos e a criptografia. Ambos são extensivamente oferecidos pelos provedores de computação na nuvem.

3.1.3. Integridade

Segunda a norma ISO/IEC 18028,

> a integridade dos dados garante com exatidão ou precisão (ou seja, os dados são processados apenas por processos autorizados ou ações de usuários autorizadas ou dispositivos) de dados. Os dados são protegidos contra modificações não autorizadas, autorizadas como atividades de exclusão, criação e replicação.

A integridade dos dados significa garantir o ACID (Atomicidade, Isolamento, Consistência e Durabilidade) da informação, que consiste em evitar perdas ou modificações por usuários não autorizados. Assim sendo, manter a integridade deve ser imposta em todos os modelos de computação em nuvem.

De acordo com (ZHOU *et al.* 2010), sistemas na nuvem devem comportar alta capacidade de processamento de dados, volumes equivalentes a Tera Bytes de dados ou até mesmo Peta Bytes. Portanto, os desafios para manter a integridade de dados estão associados à capacidade de armazenamento de dados.

3.1.4. Irretratabilidade

Segunda a norma ISO/IEC 18028,

> A irretratabilidade fornece meios técnicos para impedir que um indivíduo ou uma entidade se recusarem de ter realizado uma ação específica relacionada aos dados, fazendo prova disponível de ações em várias redes relacionadas (como prova da intenção, obrigação ou compromisso; prova da origem de dados , prova de propriedade e prova de uso de recursos). Este recurso ajuda a garantir a disponibilidade de evidências que podem ser apresentadas a um terceiro como prova técnica que de algum tipo de evento ou ação ocorreu. Métodos criptográficos são muitas vezes utilizados para a prestação de irretratabilidade.

De acordo com (RAMGOVIND *et al.* 2010), a irretratabilidade na nuvem pode ser obtida através da aplicação dos protocolos tradicionais de e-commerce de segurança e de token de provisionamento para a transmissão de dados dentro das aplicações instaladas na nuvem, como métodos de criptografia, assinaturas digitais, timestamps e serviços de confirmação de recepção de dados/mensagem (mensagens digitais que confirmam os dados enviados/recebidos).

3.1.5. Disponibilidade

Segunda a norma ISO/IEC 18028,

> A disponibilidade garante que não haja negação de acesso a elementos para uma rede autorizada, as informações armazenadas, fluxos de informação, serviços e aplicações resultantes de acontecimentos que impactam a rede.

O provedor de nuvem deve oferecer altos níveis de disponibilidade.

Os dados precisam estar sempre disponíveis quando necessário. Mesmo que o provedor da nuvem saia do mercado, esta possibilidade de ocorrência deve ser especificada através de documento de acordo (SLA-*Service Leve Agreement*).

A disponibilidade é um dos requisitos mais críticos, e é um fator que pode ser decisivo para o consumidor na escolha de um fornecedor de nuvem (disponibilidade nos modelos de serviço e de implementação na nuvem).

Um SLA é um acordo, importante no procresso de gestão de segurança, que especifica os requisitos associados à disponibilidade em serviços na nuvem e recursos entre provedor de nuvem e o consumidor.

Segundo (RAMGOVIND *et al.* 2010), durante a análise dos requisitos de segurança da informação, é importante avaliar o tipo de serviço e implementação de nuvem a ser implantado, pois alguns requisitos de segurança deverão ser obrigatórios e outros opcionais.

A figura 5 ilustra os requisitos de segurança da informação, juntamente com o modelo de serviço e de implementação de nuvem. De acordo com as diferenças dos modelos, os requisitos de segurança demarcados com "X" denotam requisitos obrigatórios e os requisitos demarcados com "*" denotam os requisitos opcionais.

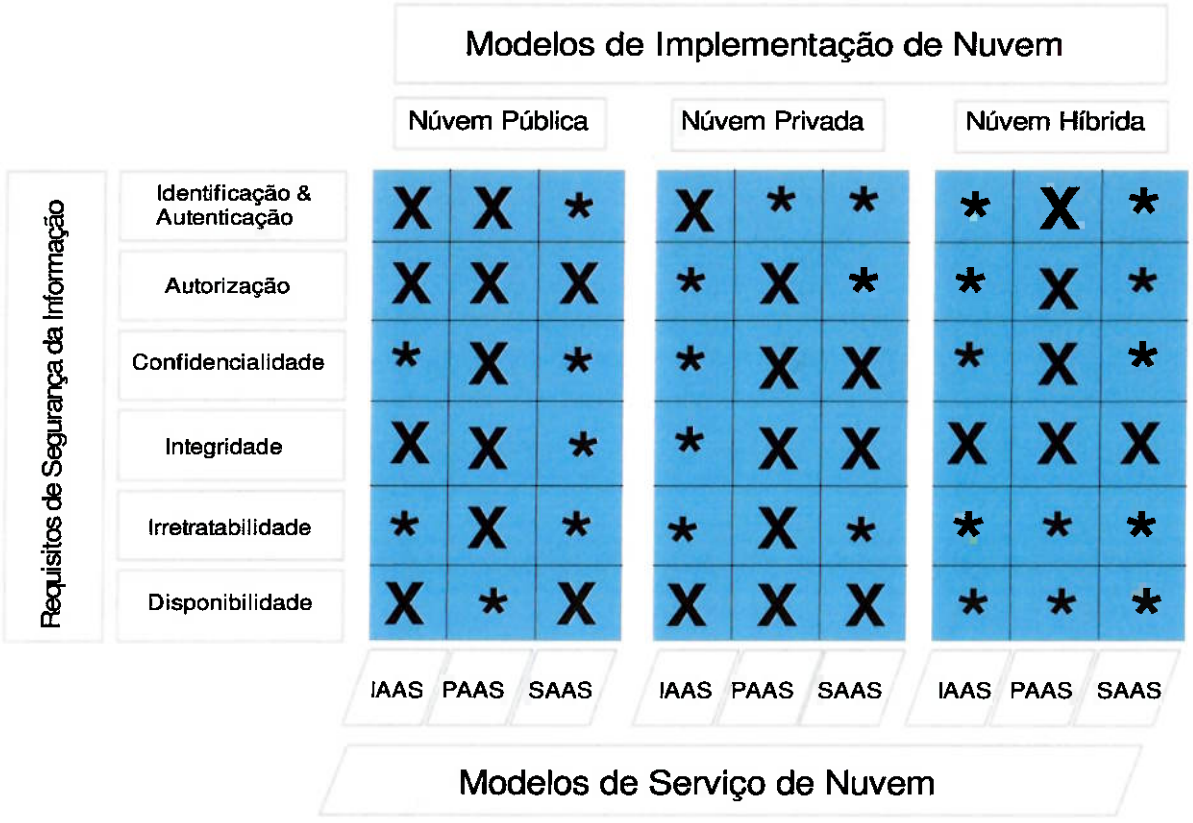

Figura 5 - Requisitos de segurança na computação em nuvem que devem ser atendidos de acordo com o tipo de modelo implantado. [Fonte: RAMGOVIND; ELOFF; SMITH E. 2010].

No contexto deste trabalho, a figura 5 será usada como um guia para avaliar o nível de segurança mais adequado a cada modelo de nuvem, neste caso divididos entre os modelos de implementação com os respectivos modelos de serviço.

Neste contexto é necessário investigar o equilíbrio ideal sobre as necessidades de negócio da empresa e avaliá-los sobre os níveis de segurança de forma a garantir o modelo de nuvem que mais se adequa, (RAMGOVIND *et al.*,2010).

4. GESTÃO DE RISCO DA SEGURANÇA DA INFORMAÇÃO NA NUVEM

Neste capítulo serão discutidos os cenários de riscos de segurança existentes a cada modelo de computação na nuvem. E posteriormente será aplicado o processo de gestão de risco de segurança da informação adaptado da norma ISO/IEC 27005.

Os cenários e a análise de risco de segurança no processo incluem a análise e avaliação dos riscos inerentes a cada modelo de nuvem, assim como, a análise e a avaliação das características dos ativos de informação a serem tratados na nuvem.

Além da análise dos modelos de nuvem, a análise sobre os ativos também faz parte do processo para decidir qual modelo de nuvem (combinação de serviço sobre um modelo de implementação) melhor se adequa e dá suporte as demandas de segurança e as características do(s) ativo(s).

Apenas como observação, para dar sequência a leitura do capítulo 4, quando mencionado o termo "ativo" refere-se às aplicações, sistemas ou dados que o cliente planeja transferir para a nuvem.

Geralmente, o ativo é tudo que é de valor para o negócio, e enquadra-se em duas classes: Dados e Aplicativos ou/e Funções e Processos (Chaves, 2011). Na computação na nuvem, ou são movimentados dados ou então são realizados processamento, envolvendo aplicativos, funções e processos.

4.1. Cenários de Riscos de Segurança da Informação na Computação na Nuvem

De acordo com Chaves (2011), é recomendado estabelecer uma abordagem sobre os cenários de risco de segurança a cada modelo de nuvem, seguindo as exigências dos requisitos de segurança da informação, esta atividade serve como auxílio para todos os atores (diretores, gestores, analistas ou provedores de serviço) no processo de avaliação de risco.

A tabela 2 mostra um exemplo de abordagem para cada requisito de segurança da informação, junto com os respectivos cenários de risco, fornecida pela *CSA (Cloud Security Alliance).*

Tabela 2 – Exemplo de uma abordagem de segurança da informação para a computação em nuvem. [Fonte: CASTRO; SOUZA. 2010].

Requisitos da Segurança	**Cenários de Risco**	**Abordagem**
Integridade	Invasões externas (*hackers ou Cyber Cloud*) aos ambientes da nuvem. Violação de leis de proteção do conteúdo dos dados.	Quais são as garantias sobre a preservação da integridade dos dados? Qual seria o impacto se algum funcionário dos provedores tivesse acesso a este ativo? Qual seria o impacto se este processo ou função fosse manipulado por um estranho? Qual seria o impacto se este processo ou função deixasse de produzir os resultados esperados Qual seria o impacto se este dado fosse modificado de forma inesperada?
Confidencialidade	Existência de diversos usuários instalados nos mesmos sistemas de armazenamento.	Como é realizada a segregação de dados? Como é protegida a propriedade intelectual e segredos comerciais? Qual seria o impacto se este ativo se tornasse de conhecimento público? Há políticas e procedimentos estabelecidos e medidas implementadas para limitar o acesso a dados confidenciais a partir de dispositivos móveis e portáteis?
Disponibilidade	Recuperação de dados gerenciados por terceiros.	Como é garantida a arquitetura de disponibilidade? Qual seria o impacto se este ativo se tornasse indisponível por um determinado período de tempo? A recuperação de informações críticas está sujeita a atrasos?
Autenticidade (autenticação e	Verificação da autenticidade das entidades comunicantes.	Que recursos são utilizados na autenticação e controle de acesso dos usuários? Há controles vigentes para impedir o acesso

autorização)		não autorizado ao código-fonte de seu aplicativo, programa ou objeto? E como garantir que seja restrito somente à equipe autorizada?
Irretratabilidade	Auditoria das ações executadas por usuários no sistema.	Os usuários do modelo são capazes de negarem suas ações? Há formas para restringir, registrar e monitorar o acesso aos sistemas de gerenciamento de segurança da informação?

Uma vez identificado os riscos referentes a cada requisito de segurança da informação, é importante também identificar e classificar os riscos referentes aos modelos de computação na nuvem.

Conforme detalhado em capítulos anteriores deste trabalho, os modelos de computação na nuvem podem ser considerados como sendo composto por três modelos de serviço, sendo IaaS, PaaS e SaaS, e quatro modelo de implementação, sendo as estruturas de nuvem pública, privada, comunitária ou hibrída. E para cada tipo de modelo de serviço e implementação existe uma classificação de risco associado. A tabela 3 ilustra os riscos referentes aos modelos de serviço na computação em nuvem.

Tabela 3 – Riscos referentes aos modelos de serviços na nuvem.
[Fonte: CASTRO; SOUZA. 2010].

Modelos de Serviço de Computação na Nuvem		
Modelo de Serviço	**Características de Risco**	**Classificação de risco**
Infraestrutura como Serviço (*IaaS*)	O consumidor não administra ou controla a infraestrutura da nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento de aplicativos implantados, e os componentes de rede selecionados. Deve-se considerar: Opções para minimizar o impacto se o provedor de nuvem tiver alguma interrupção de serviço.	Médio
Plataforma como Serviço (PaaS)	O consumidor não administra ou controla os recursos de infraestrutura da nuvem subjacente, tais como componente de rede, servidores, sistemas operacionais, ou armazenamento. O consumidor tem controle sobre os aplicativos utilizados na hospedagem de aplicativos e nas configurações de ambientes. Deve considerar: • Incompatibilidade de integração com outras	Alto

	plataformas. • Dependência dos recursos de um único provedor.	
Software como serviço (SaaS)	O consumidor não administra ou controla a infraestrutura subjacente o que inclui componentes de rede, servidores, sistemas operacionais, armazenamento ou capacidade de aplicação. Deve-se considerar: • Quem possui as aplicações? • Onde as aplicações residem? • Incompatibilidade de integração com outras plataformas. • Dependência dos recursos de um único provedor.	Muito Alto

A seguir, na tabela 4, é ilustrado os riscos referentes aos modelos de implementação na computação em nuvem.

Tabela 4 – Riscos referente aos modelos de implementação na nuvem.

[Fonte: ISACA, 2009].

Modelos de Implementação de Computação na Nuvem		
Modelo de Implementação	**Características do Risco (global)**	**Classificação de risco (global)**
Nuvem Privada	Serviços em nuvem com risco mínimo. Não pode fornecer a escalabilidade e agilidade dos serviços de nuvem pública. Comparado com outros modelos de implementação de nuvem, esse modelo é o que prover um menor risco, devido de sua natureza privada. E, embora traga algumas facilidades por estar no ambiente da empresa, é exigido um gerenciamento interno, o que diminui a economia de recursos. Além disso, por estar diretamente atrelado aos processos corporativos, torna-se engessado em termos de automação de tarefas como atualizações. **Risco**: Possibilidade de falta de escalabilidade de recursos computacionais quando o volume de acesso for elevado, e o alto cusco financeiro com gerenciamento interno.	Baixo
Nuvem Comunitária	Segue o conceito parecido com o modelo de nuvem privada. A definição de políticas de acesso e a utilização de tecnologias de autenticação e autorização são semelhantes ao modelo privado. Outro fator que merece destaque é o fato dos dados estarem armazenados junto com os dados de outros concorrentes pertencentes à comunidade. **Risco**: Possibilidade da falta de escalabilidade de recursos computacionais quando o volume de acesso for muito elevado.	Médio
	O modelo é disponibilizado para o público em geral ou para	

Nuvem Pública	grupos de indústrias, sendo acessado por qualquer usuário que conheça a localização do serviço. Por isso não podem ser aplicadas restrições de acesso quanto ao gerenciamento de redes, e menos ainda, aplicar técnicas de autenticação e autorização. O modelo proporciona as organizações mais economia de escala, uma vez que compartilha os recursos, por outro lado, possui limites de customização relacionados justamente à segurança das informações, SLAs e políticas de acesso, uma vez que os dados podem ser armazenados em locais desconhecidos e não podem ser facilmente recuperável. **Riscos**: Possibilidade de Violação de confidencialidade, o desconhecimento da localização e da segregação dos dados.	Alto
Nuvem Híbrida	A adoção do modelo exige uma minuciosa classificação e rotulagem dos dados, para garantir que os mesmos estão sendo atribuídos ao tipo de nuvem correto. **Riscos:** O alto risco agregado, devido à fusão entre os diferentes modelos de implementação e o risco que os acompanham.	Alto

Como se pode observar, os riscos são diferentes para cada modelo e é importante destacar que, ao considerar diferentes tipos de serviços e modelos de implementação, as empresas devem considerar os riscos que os acompanham.

Dada a classificação global de risco de segurança, o modelo IaaS e o modelo de nuvem privada apontam como de menor risco (comparado com os demais modelos de serviço e implementação respectivamente), por outro lado esses modelos (combinação entre IaaS em nuvem privada) nem sempre é a melhor solução para o ativo passível de transferência para a nuvem, e por este motivo antes de adotar um modelo de serviço e de implementação, é necessário avaliar as características do ativo do cliente e diagnosticar à qual serviço melhor se aplica.

O cliente precisa saber das aplicabilidades e atentar-se aos pontos de atenção referente a cada modelo de serviço (conforme explorados no capítulo 2) para auxiliar na melhor definição e escolha apropriada para o ativo analisado.

4.2. Processo de Gestão de Risco na Computação na Nuvem

De acordo com o processo de gestão de risco da norma ISO/IEC 27005 (ilustrado na figura 4) e do ciclo de melhoria contínua (conforme a figura 3), é recomendado que o consumidor siga um roteiro para entender o processo de gestão de risco e a maneira

como este dever ser construído (Chaves, 2011). Conforme abordado no capítulo 2, para aplicar um processo de gestão de risco de segurança da informação na nuvem, é necessário adaptar a norma ISO/IEC 27005 para atender as necessidades, políticas e cultural do cliente consumidor.

A figura 6 mostra um processo de gestão de risco de segurança que devem ser aplicados aos ativos de informação, adaptado da norma ISO/IEC 27005, para auxiliar no processo de decisão de escolha de um provedor de nuvem.

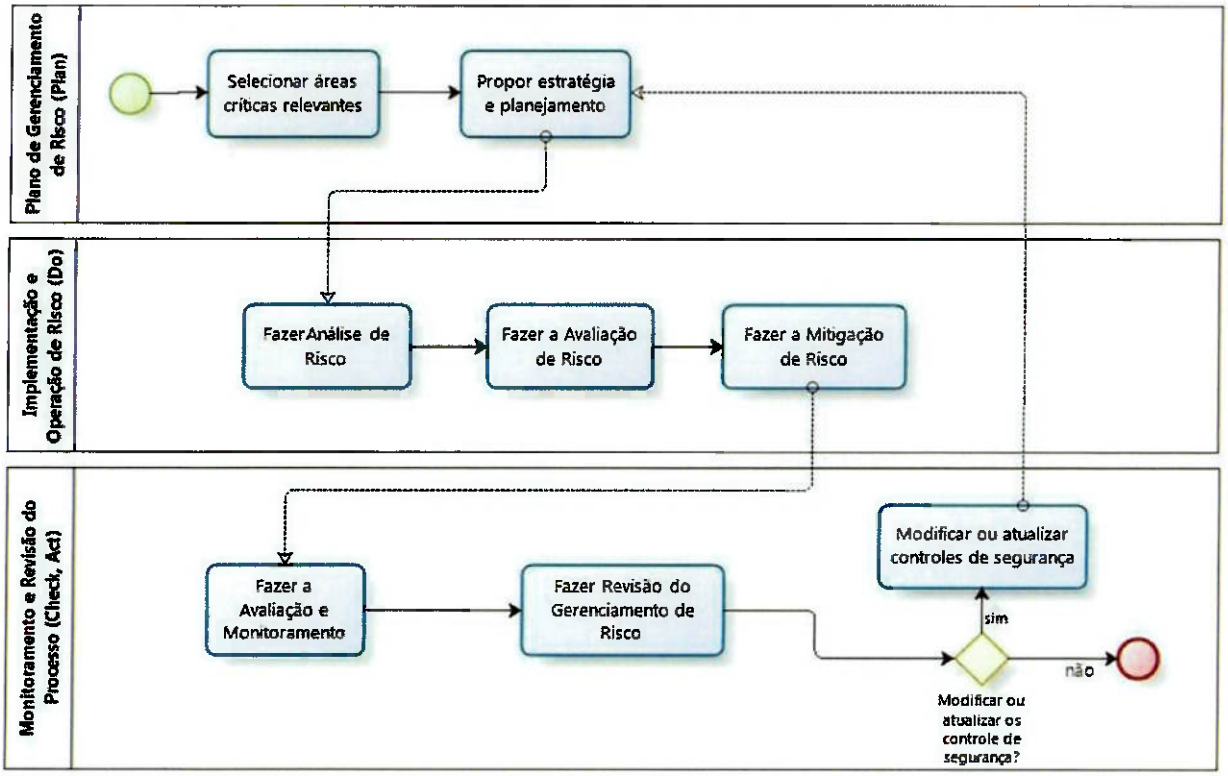

Figura 6 - Processo de gestão de riscos aplicado aos ativos passíveis de transferência para a nuvem.

O processo é composto por sete etapas, seguindo o ciclo PDCA:

No *Plan:* selecionar áreas críticas relevantes, propor uma estratégia e planejamento para dar um direcionamento na gestão de risco sobre os ativos de informação. No *Do:* fazer análise de risco da segurança da informação, avaliar os riscos inerentes aos modelos de nuvem, mitigar os riscos identificados. No *Check e Act:*, fazer o programa de avaliação e monitoramento de risco e a revisão, e gestão de risco.

O processo de gestão dos riscos existe devido a constante surgimento de novas ameaças sujeitas a explorar as vulnerabilidades dos ativos de informação, o que exige que se tomem algumas medidas de prevenção.

4.2.1. Estabelecer um Plano de Gestão de Risco (*Plan*)

Para estabelecer um plano de gestão de risco é necessário seguir duas etapas do processo: seleção de áreas críticas relevantes, estratégia e planejamento, conforme ilustrado na tabela 7 abaixo:

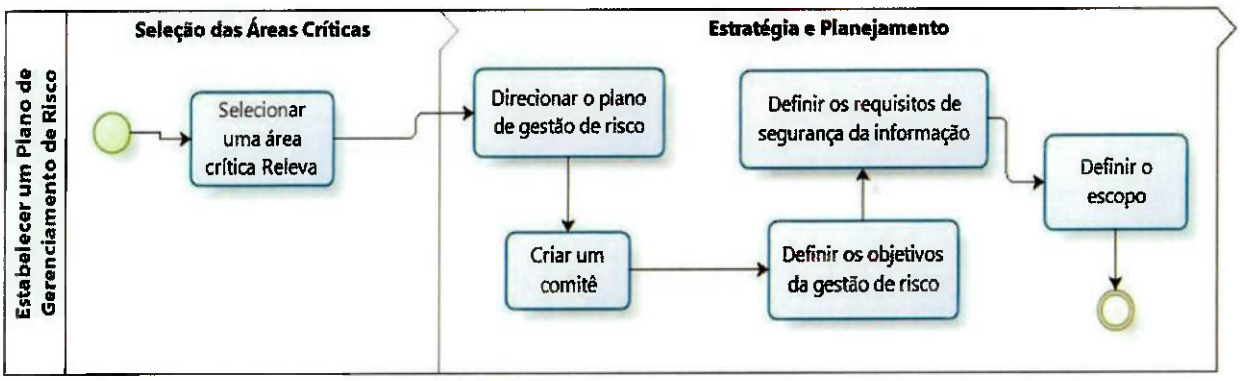

Figura 7 - Primeira fase do processo de gestão de risco de segurança.

4.2.1.1 Seleção de Áreas Críticas Relevantes

De acordo com (Zhang *et al.* 2010), para seleção de áreas críticas, são destacados doze domínios críticos para a computação em nuvem, e estes são ajustados para atender os requisitos de segurança da informação de maneira estratégica dentro dos modelos (de serviço e de implementação) na nuvem.

Na figura 8 são destacados esses domínios:

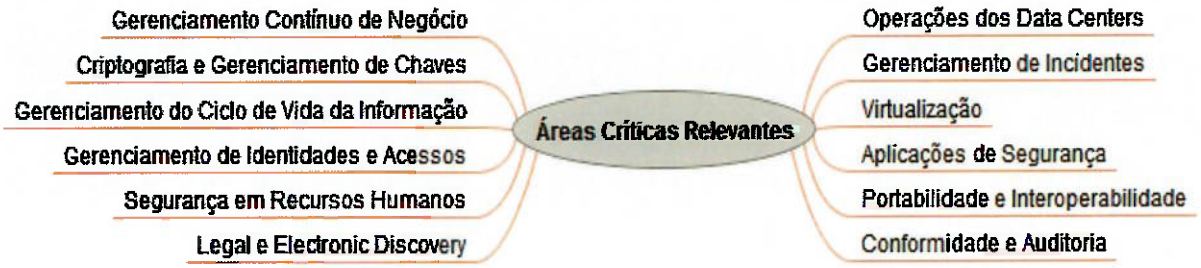

Figura 8 - Domínios críticos relevantes extraídos do guia da *CSA* para a segurança na computação na nuvem.

Esta etapa abrange o entendimento de todos os modelos de serviços e implementação de nuvem (de acordo com as figuras 1 e 2) juntamente com os domínios mostrados na figura 8.

Nesta etapa, deve-se selecionar uma área crítica relevante, por exemplo:

Para um provedor de *SaaS*, a segurança está focada nas aplicações, no gerenciamento de controle de acesso, na criptografia ou no gerenciamento de chaves para análise, na avaliação de ameaças e nos riscos de vulnerabilidades para o cliente consumidor.

4.2.1.2 Estratégia e Planejamento (*Plan*)

A proposta nesta etapa é:

- Estabelecer um direcionamento na gestão de risco de segurança e um guia de atividades;
- Criar um comitê para discutir ou debater os aspectos de segurança;
- Definir os objetivos da gestão de risco, os requisitos de segurança da informação e o escopo.

De acordo com (Zhang *et al.*,2010), essa etapa é realizada em conjunto com as áreas críticas relevantes para garantir os planos de comunicação onde são especificados claramente os papéis e as responsabilidades dos envolvidos, a identificação das áreas críticas de foco, e fornecer opções para a alocação de recursos e otimização.

4.2.2. Implementação e Operação de Risco (*Do*)

Esta etapa envolve três processos: análise de risco, avaliação de risco e mitigação de risco. Conforme ilustrado na figura 9:

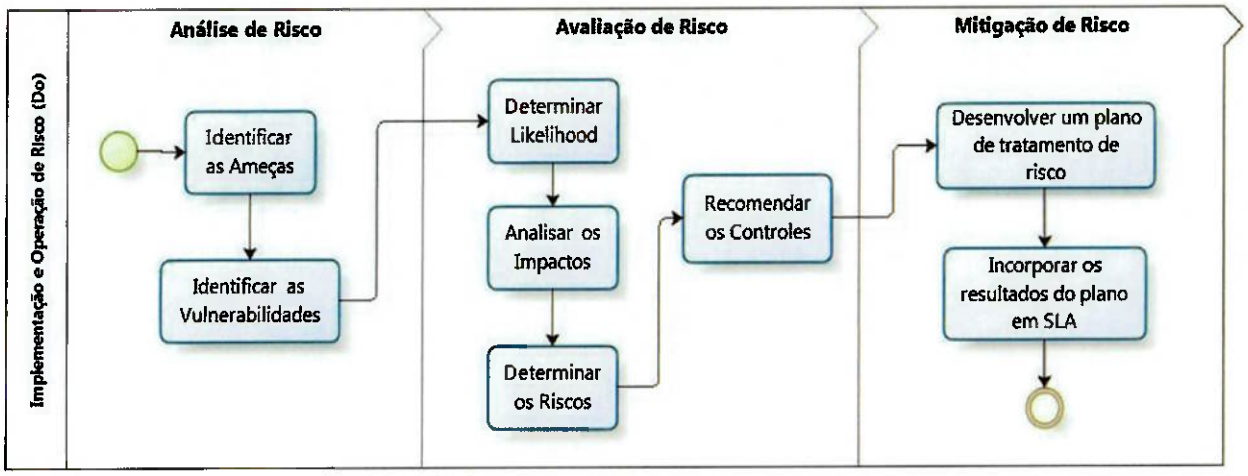

Figura 9 - Segunda fase do processo de gestão de risco de segurança.

Os resultados da análise dos riscos (*output* do processo de análise e *input* para o processo de avaliação e mitigação de risco) deverão ajudar a direcionar e determinar quais as ações de controle é mais apropriado para a mitigação e controle dos riscos.

A avaliação dos riscos (*input* para o processo de mitigação de risco) deve ser feita tendo em conta uma análise de custo/benefício, para revelar se compensa um risco ser minimizado ou transferido.

4.2.2.1 Análise de Risco

Uma vez estabelecido o plano de gestão de risco e a identificação e avaliação dos ativos envolvidos e passíveis de transferência para a nuvem, a análise de risco segue em duas atividades: Identificação de ameaças e Identificação das vulnerabilidades, (Zhang *et al.* 2010).

- **Identificação das Ameças**

  Por exemplo, a capacidade de invasão e exploração de hackers nos componenetes de infraestrutura, nos serviços de rede e de aplicações indica uma vulnerabilidade, sendo uma grande ameaça para os modelos de nuvem,

principalmente para os modelos de serviço IaaS e PaaS, cujas responsabilidades de gerenciamento de segurança (indentificação de vulnerabilidades e configurações) permanecem com o cliente consumidor, (Zhang *et al.* 2010).

A tabela 5 apresenta um exemplo da etapa de identificação de ameaças:

Tabela 5 – Exemplo de identificação de ameaças [Fonte: ZHANG; WUWONG; LI; ZHANG, 2010.]

Fonte da ameaça	**Motivação**	**Ações de ameaça**
Ações de Hackers e Crackers	Desafios, ego ou rebelião.	Por invasão do sistema e acesso não autorizado.
Computação Criminosa	Destruição de informações, divulgações de informações ilegais, ganho monetário ou alteração de dados não autorizados.	Criminalidade via computador (por exemplo: perseguição), ações fraudulentas (por exemplo: repetição, representação ou interceptação da informação), informações de suborno, sistema de invasão.
Terrorismo	Por chantagem, destruição, exploração ou vingança.	Bomba, terrorismo, guerra por informação, ataque, invasão e violação de sistemas.

A figura 10 é um exemplo de entradas e saídas desta etapa:

Figura 10 – Entrada e saída da etapa de Identificação de Ameaças.

- **Identificação das Vulnerabilidades**

A vulnerabilidade é um fator importante de risco, e sua identificação é essencial na proteção dos componentes de infraestrutura (como: hosts,

despositivos de rede e aplicações) de ataques contra as vulnerabilidades já conhecidas.

A tabela 6 apresenta um exemplo de identificação de vulnerablidades para a redução ou eliminação dos riscos durante o processo de mitigação de risco.

Tabela 6 - Exemplo de Identificação de Vulnerabilidades. [Fonte: ZHANG; WUWONG; LI; ZHANG, 2010]

Vulnerabilidade	Fonte da ameaça	Ações da ameaça
Identificação de funcionários desligados da organização que ainda não foram removidos do sistema de acesso.	Funcionários desligados.	Conectar na rede e acessar os dados de propriedade da empresa.
Firewall da empresa permite telnet de entrada, e ID de hóspedes está habilitado no servidor.	Usuários não autorizados.	Usando telnet de conexão para acessar servidores e navegar no sistema de arquivos com uma identificação de usuário hóspede.
O fornecedor tem identificação falha no projeto de segurança do sistema; E novas correções não foram aplicadas ao sistema.	Usuários não autorizados.	Obtendo acesso não autorizado a arquivos confidenciais baseado nas vulnerabilidades conhecidas identificadas no sistema.

Os métodos recomendados para a identificação de vulnerabilidades de sistemas se aplicam às fontes (origem) das vulnerabilidades, no desempenho de testes de segurança de sistemas, e no desenvolvimento de uma lista de verificação dos requisitos de segurança da informação.

A figura 11 é um exemplo de entradas e saídas desta etapa:

Figura 11 – Entrada e saída da etapa de Identificação de Vulnerabilidades.

4.2.2.2 Avaliação de Risco

A avaliação de risco é a determinação quantitativa e qualitativa do processo de análise de risco. Nesta etapa, são realizadas quatro atividades: Definição das Probabilidades (*Likelihood*) de ocorrência eventos de risco, Análise de Impacto, Definição dos Níveis de Riscos e Recomendações de Controle.

- **Definição das Probabilidades (*Likelihood*)**

  Esta atividade consiste numa classificação geral que indica o nível de probabilidade de ocorrência de um ou mais eventos nocivos (isto é, de vulnerabilidade) de acordo com as fontes das ameaças identificadas.

  Como resultado desta atividade tem-se a classificação do nível de probabilidade em alto, médio e baixo, conforme a tabela 7:

Tabela 7 - Definição de probabilidade. [Fonte: ZHANG; WUWONG; LI; ZHANG, 2010]

Nível de probabilidade	Definição da probabilidade
Alto	A fonte da ameaça é altamente motivada e suficientemente suscetível, e controles para evitar a vulnerabilidade devem ser exercidos de forma eficaz.
Médio	A fonte de ameaça é motivada e suscetível, mas controles estão em vigor para impedir o exercício da vulnerabilidade.
Baixo	A fonte de ameaça carece de motivação ou capacidade, e controles estão em vigor para evitar, ou pelo menos impedir a vulnerabilidade de ser exercida.

A figura 12 é um exemplo de entradas e saídas desta etapa:

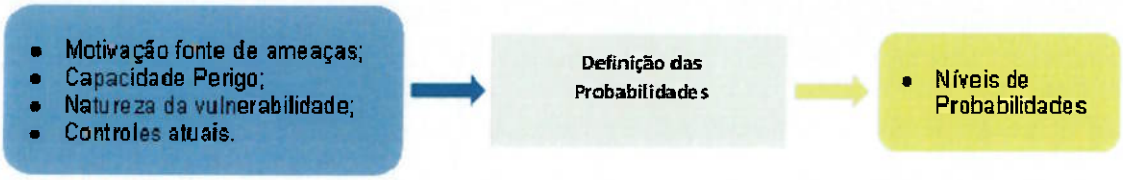

Figura 12 – Entrada e saída da etapa de Definição das Probabilidades.

- **Análise de Impacto**

Esta atividade consiste em determinar o nível de impacto negativo causado pelas ameaças e vulnerabilidades nos ativos.

O impacto negativo pode ser descrita em termos de perda ou degradação de qualquer, ou a combinação de alguns, dos seguintes objetivos de segurança da informação: integridade, disponibilidade, confidencialidade e estes podem ser classificados qualitativamente como alto, médio e baixo. A tabela 8 apresenta os níveis de impacto conforme (Zhang *et al.* ,2010):

Tabela 8 - Níveis de impacto. [Fonte: ZHANG; WUWONG; LI; ZHANG, 2010]

Nível do Impacto	Definição do Impacto
Alto	O exercício sobre a vulnerabilidade pode resultar na perda, de alto custo, dos ativos ou de recursos; Pode significativamente violar, prejudicar ou impedir a missão de uma organização, a sua reputação ou interesse.
Médio	O exercício sobre a vulnerabilidade pode resultar na perda custosa de ativos ou de recursos; Pode violar, prejudicar ou impedir a missão de uma organização, a sua reputação, ou interesse.
Baixo	O exercício sobre a vulnerabilidade pode resultar na parte de alguns ativos ou recursos, ou pode afetar visivelmente a missão de uma organização, a reputação, ou interesse.

A análise de impacto negativo de cada ativo é feita através de questionários. Exemplos de algumas destas questões estão relacionadas a seguir (Chaves, 2011):

- Qual seria o impacto se este ativo se tornasse de conhecimento público?
- Qual seria o impacto se algum funcionário dos provedores tivesse acessa a este ativo
- Qual seria o impacto se este processo ou função deixasse de produzir os resultados esperados?
- Qual seria o impacto se este dado fosse modificado de forma inesperada?
- Qual seria o impacto se este ativo se tornasse indisponível por um período de tempo?

Essencialmente, o objetivo das questões acima é avaliar os requisitos de segurança da informação dos ativos (conforme mostrado na tabela 2) e como estes requisitos podem ser afetados se todos ou parte dos ativos do consumidor sofrer algum tipo de manipulação ou acesso não autorizado na nuvem.

A figura 13 é um exemplo de entradas e saídas desta etapa:

Figura 13 – Entrada e saída da etapa de Análise de Impacto.

- **Definição dos Níveis de Risco**

  Conforme (Zhang *et al.*, 2010), os níveis de risco são definidos pela probabilidade de ameaça atribuída a cada nível de impacto. A tabela 9 mostra como os níveis de risco são derivados.

Tabela 9 - Definição dos níveis de risco. [Fonte: ZHANG; WUWONG; LI; ZHANG, 2010]

Probabilidade de Ameaça	**Nível de Impacto**		
	Baixo **(10)**	Médio **(50)**	Alto **(100)**
Alto **(1.0)**	Baixo 10 x 1.0 = 10	Médio 50 x 1.0 = 50	Alto 100 x 1.0 = 100
Médio **(0.5)**	Baixo 10 x 0.5 = 5	Médio 50 x 0.5 = 25	Alto 100 x 0.5 = 50
Baixo **(0.1)**	Baixo 10 x 0.1 = 1	Médio 50 x 0.1 = 5	Alto 100 x 0.1 = 10

A finalidade desta definição é encontrar uma classificação global de risco a ser aplicado sobre os modelos de nuvem, e as oportunidades que impactam as áreas críticas de risco (selecionadas na primeira fase do processo de gestão de risco – Seleção de Áreas Críticas Relevantes).

A tabela 10 descreve os níveis de risco mostrados na Tabela 9, assim como as ações necessárias para cada nível:

Tabela 10 - Descrição de risco e ações necessárias. [Fonte: ZHANG; WUWONG; LI; ZHANG, 2010]

Nível de Risco	**Descrição do Risco e as Ações Necessárias**
Alto	Se a análise é classificada com risco elevado, existe uma forte necessidade de medidas corretivas. Um sistema pode continuar a funcionar, porém um plano de ação corretiva deve ser aplicado o mais rápido possível.
	Se a análise é classificada com risco médio, ações corretivas são necessárias e um plano deve ser desenvolvido para incorporar essas ações dentro de um prazo razoável de

Médio	tempo.
Baixo	Se a análise é classificada com baixo risco, gerentes ou responsáveis devem determinar se ações corretivas serão necessárias ou decidir por aceitar o risco.

A figura 14 é um exemplo de entradas e saídas desta etapa:

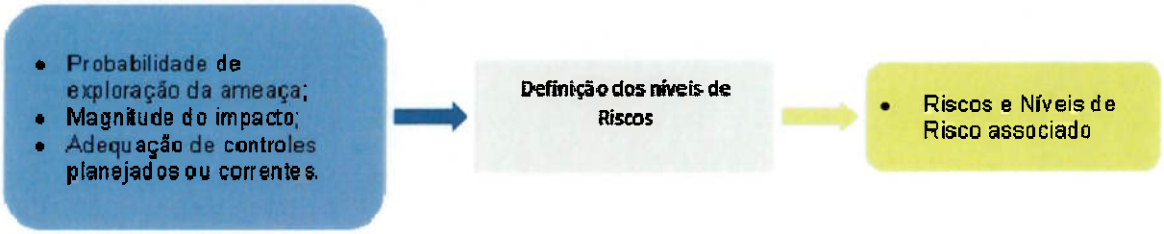

Figura 14 – Entrada e saída da etapa de Definição dos Níveis de Risco.

- **Recomendações de Controle**

  O objetivo dos controles é a redução no nível de risco para o ambiente de computação na nuvem para um nível aceitável.

  Conforme (Zhang *et al.* 2010), ao recomendar controles e soluções alternativas para reduzir ou eliminar os riscos identificados, devem-se consideradar alguns fatores:

  - Implementar e manter um programa de segurança;
  - Construir e manter uma infraestrutura de nuvem segura;
  - Assegurar a proteção de dados confidenciais;
  - Implementar o acesso e gerenciamento de identidade;
  - Estabelecer o provisionamento.
  - Implementar governança e gestão de segurança
  - Implementar a auditoria para o gerenciamento de vulnerabilidades
  - Manter um ambiente de teste e validação.

4.2.2.3 Mitigação de Risco

Na etapa de mitigação de risco, o provedor de nuvem deve desenvolver um plano de tratamento de risco (RTP) com múltiplas opções, como: transferência, evasão, retenção, redução e aceitação. (Zhang *et al.*, 2010).

Os resultados do plano de mitigação de riscos devem ser incorporados em acordos de serviço (SLA), porque os diferentes modelos de computação na nuvem têm várias maneiras para mitigação de vulnerabilidades e ameaças.

Nesta etapa, o consumidor tem um entendimento da importância dos ativos envolvidos e dos riscos de segurança que os acompanham. Desta forma pode-se então determinar quais modelos (modelos de serviço e de implementação) de computação na nuvem são mais adequados e se os riscos referentes a cada um dos modelos (conforme mostrado nas tabelas 3 e 4) são aceitáveis para o negócio do consumidor.

4.2.3. Monitoramento e Revisão do Processo (*Check, Act*)

Após a etapa de mitigação de risco, o provedor de nuvem, inicia o acompanhamento como parte da avaliação integral e contínua de segurança sobre os ativos. Nesta etapa é feita o monitoramento e a revisão de todo o processo de gestão de risco de segurança na nuvem, conforme ilustrado na figura 15 a seguir:

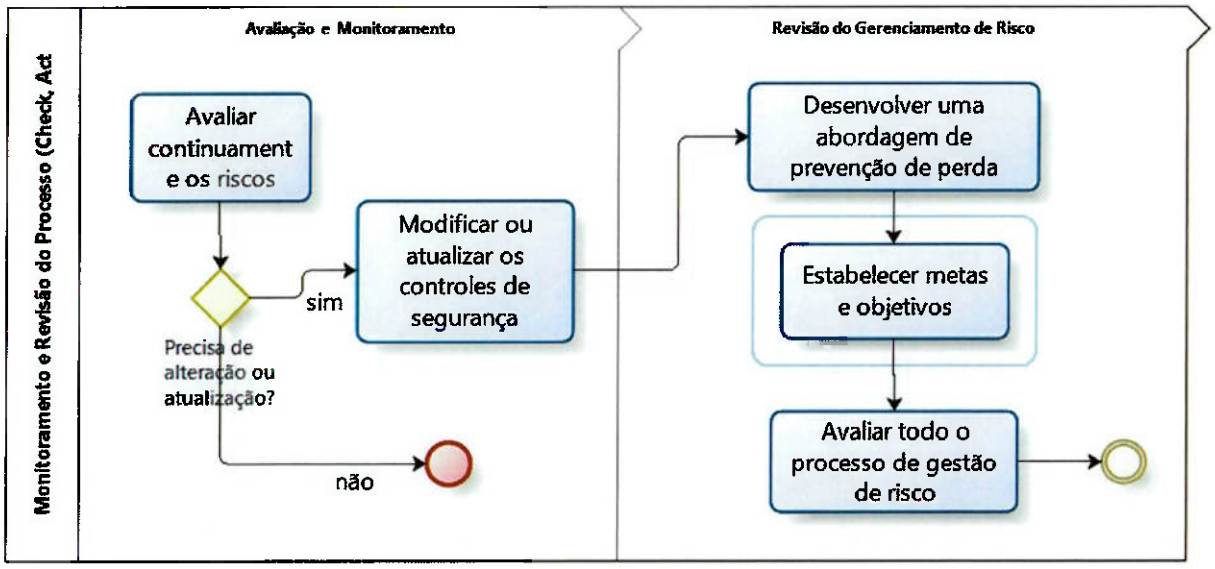

Figura 15 - Terceira fase do processo de gestão de risco de segurança.

4.2.3.1 Avaliação e Monitoramento

O cliente consumidor inicia o acompanhamento sobre as atividades da gestão de risco como parte de um programa de monitoramento contínuo. O programa inclui a avaliação contínua dos riscos para determinar se há a necessidade de alterar ou atualizar o atual conjunto de controles de segurança. Existem momentos em que alguns eventos desencadeiam a necessidade imediata de avaliar as condições de segurança do sistema de informação (um ou mais ativos) e, se necessário, modificar os controles de segurança. (Zhang *et al.*, 2010)

4.2.3.2 Revisão da Gestão de Risco

A finalidade das revisões na gestão de risco é contribuir para o desenvolvimento de uma abordagem destinada a prevenção de perda de dados e adquirir melhor controle de segurança. O objetivo é estabelecer uma base para definir metas, objetivos e avaliação de todo o processo de gestão de risco de segurança.

De acordo com MILLER (2009), encontrar os principais objetivos no processo de gestão de risco de segurança, incluem basicamente:

- Estabelecer um plano para proteção da informação baseado em ativos e em Planos de Mitigação de Riscos;
- Reforçar a capacidade da organização para selecionar e aplicar a proteção baseada no risco específico e nas ameaças que afetam um determinado ativo;
- Assegurar que a metodologia de gestão de risco de segurança está sendo utilizada em toda organização.

De acordo com o guia da *CSA*, é de fundamental importância que os processos de negócio e procedimento considerem os aspectos de segurança, principalmente ao adotar o modelo de computação na nuvem. Além disso, os gestores de segurança da informação precisam ajustar suas políticas e procedimentos de segurança para atender às necessidades de negócio para um modelo de computação na nuvem.

Neste capítulo, foi apresentado o processo de gestão de risco de segurança da informação na computação na nuvem, abordando as etapas (adaptadas da norma ISO/IEC 27005) como a seleção das áreas críticas relevantes, o planejamento e estratégia para estabelecer um direcionamento da gestão de risco, a análise de risco (vulnerabilidades identificadas), a avaliação de risco que inclui a identificação de probabilidades e ameaças, os impactos de segurança da informação e dos níveis de riscos associados. Em seguida o plano de mitigação de risco para redução ou aceitação do risco de segurança, o programa de avaliação e monitoramento do processo de gestão de risco de segurança da informação na nuvem e a sua revisão para atualizações e melhorias da gestão foram descritas.

5. CONSIDERAÇÕES FINAIS

Neste trabalho foram abordados as características dos modelos de serviços e de implementação de computação na nuvem e seus respectivos riscos de segurança.

Nos aspectos de segurança foram destacados os requisitos de segurança da informação da norma ISO/IEC 18028, e em seguida foram mostradas, passo a passo, as etapas do processo de gestão de risco de segurança para atender os requisitos de segurança da informação que devem ser aplicadas aos ativos passíveis de transferência para a nuvem do cliente consumidor.

O tema central neste trabalho foi apresentar uma adaptação da norma ISO/IEC 27005 no processo de gestão de risco de segurança da informação aos modelos de serviço e implementação de computação em nuvem, visando atender os requisitos de segurança, segundo a ISO/IEC 18028, dos ativos passiveis de transferência para a nuvem.

Vimos que nos aspectos de segurança da informação as questões pertinentes não diferem do conceito de segurança que deve ser aplicado em cada um dos modelos de serviço e de implementação de computação na nuvem.

Ao migrar ativos de informação do cliente consumidor para um ambiente na nuvem, gerentes ou responsáveis devem investir na melhoria do processo de segurança, implantar ferramentas e controles de segurança, para identificação, análise e mitigação de riscos. Embora este trabalho não trate de governança, muitas referências apontam pela necessidade de adotar um modelo de governança da segurança da informação para estabelecer regras, políticas, controle e manutenção sobre os ativos de informação e dos riscos inerentes dos modelos prestados na nuvem.

Contudo, é importante considerar que muitas vezes os procedimentos de segurança do provedor, para a garantia de confidencialidade e integridade de dados, são mais adequados do que de muitas empresas, principalmente empresas de médio e pequeno porte.

Como a computação em nuvem ainda está no início de sua evolução tecnológica e o mercado ainda é incipiente, o cenário futuro deverá ser bem diferente do contexto atual. E os provedores estão preparados para utilizar os padrões mais atuais de segurança, seja em confidencialidade de informação ou integridade da mesma.

Contudo, o cliente também deve ter processos seguros de manuseio e administração dessa informação.

6. REFERÊNCIAS

CASTRO R. C. C.; SOUSA P., Segurança em Cloud Computing: Governança e Gerenciamento de Riscos de Segurança, In: III Congresso Tecnológico de TI e Telecom InfoBrasil 2010, Anais Eletrônicos; Fortaleza, CE, 2010. Disponível em http://www.infobrasil.inf.br/userfiles/26-05-S5-1-68740-Seguranca%20em%20Cloud.pdf.

CHAVES S.; A Questão dos Riscos em Ambientes de Computação em Nuvem. 2011. 140f. Dissertação (Pós-Graduação em Administração) - Departamento de Administração da Faculdade de Economia, Administração e Contabilidade da Universidade de São Paulo, São Paulo, 2011.

Cloud Security Alliance (CSA). (2012). Disponível em: http://www.cloudsecurityalliance.org/. Acessado em Setembro de 2012.

GROBAUER, B.; WALLOSCHEK, T.; STOCKER, E., *Understending Cloud Computing Vulnerabilities*, 2011 Copublished By the IEEE Computer and Reliability Societies. Disponível em: www.computer.org/security. Acessado em Março de 2013.

ISACA, Emerging Technology – "Cloud Computing: Business Benefits with Security, Governance and Assurance Perspectives." – ISACA, Illions, USA – Oct, 2009. Disponível em http://www.isaca.org. Acessado em Dezembro de 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) ISO/IEC 27001:2006 – Information technology – Security techniques – Code of practice for information security management. Geneva: ISO, Mar/2006.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) ISO/IEC 27005:2008 – Information Technology – Security techniques – Information Security risk managment. Geneva: ISO, Jun/2008.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) ISO/IEC 18028:2006 – Information Technology – Security techniques – IT network security - Geneva: ISO, Feb/2006.

IsecT, The Information Portal for ISO 27001, jan. 2012. Disponível em <http://www.iso27001security.com/html/27001.html>. Acesso em: 18/12/2011.

MELL, P.; GRANCE, T., The NIST Definition of Cloud Computing. Version set. 2011. Disponível em: http://csrc.nist.gov/publications/nistpubs/800-145SP-800-145.pdf Acesso em: 18/12/2012.

MILLER, J.; CANDLE, L.; WALD, H., - Information Security Governance: Government Considerations for the Cloud Computing Environment, August 2009 – USA. Disponível em http://boozallen.com/publications. Acessado em Dezembro de 2012.

RAMGOVIND S.; ELOFF MM.; SMITH E., *The Management of Security in Cloud Computing*, Information Security for South Africa (ISSA), 2010.

TAURION, C. Cloud Computing: Transformando o Mundo do TI. 1a Ed., Editora Brasport, Rio de Janeiro, RJ – 2009.

WEN-HSI L. H., *Conceptual Framework of Cloud Computing Governance Model – An Education Perspective,* IEEE TECHNOLOGY AND ENGINEERING EDUCATION (ITEE), 2012.

ZHANG X.; WUWONG N.; LI H.; ZHANG X.,*Information Security Risk Management Framework for the Cloud Computing Environments*, 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010).

ZHOU M.; ZHANG R.; XIE W.; QIAN W.; ZHOU A., *Security and Privacy in Cloud Computing: A Survey,* 2010. SKG '10 Proceedings of the 2010 Sixth International Conference on Semantics, Knowledge and Grids, pgs. 105-112, IEEE Computer Society Washington DC. 2010.