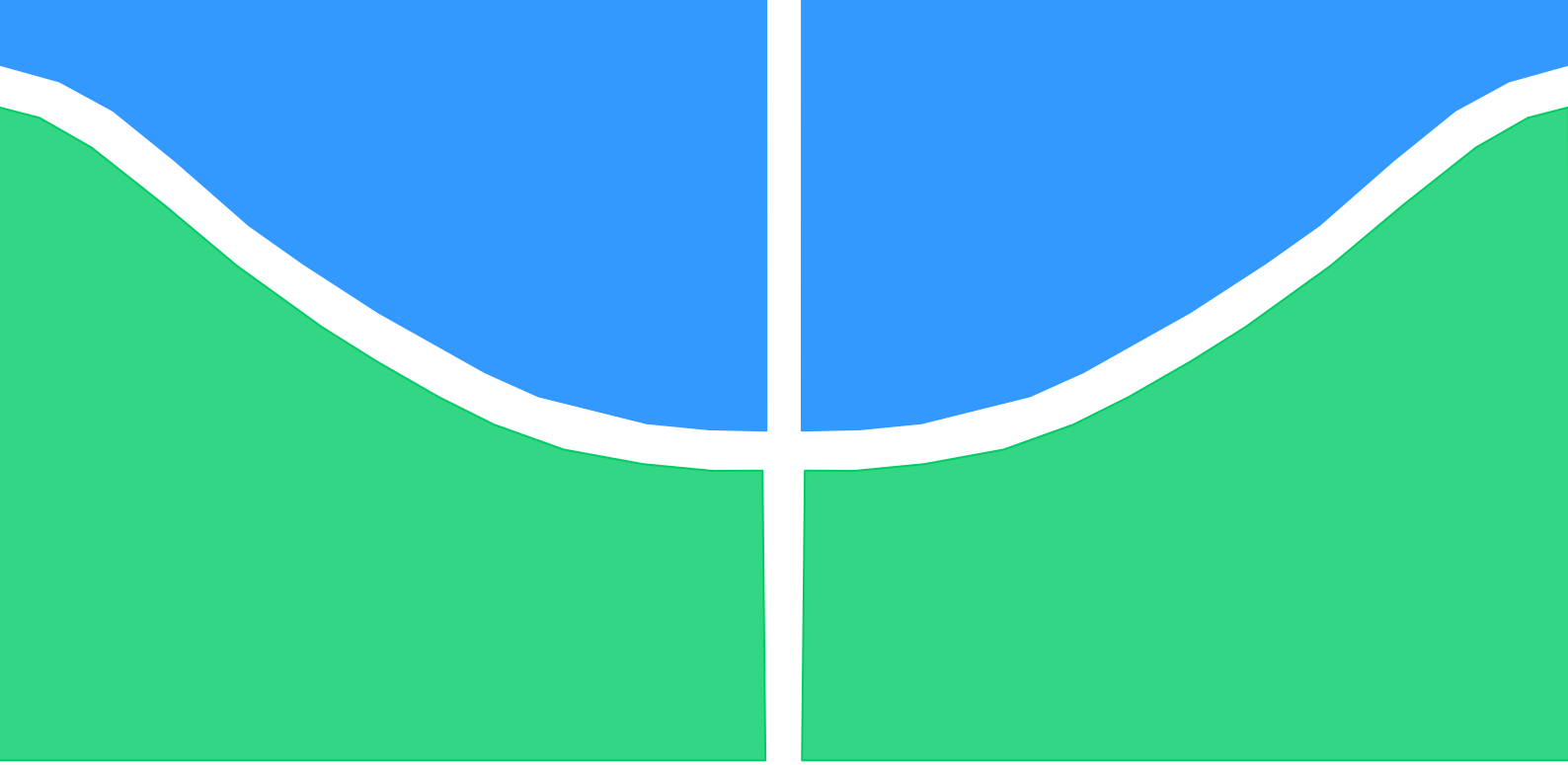

TRABALHO DE GRADUAÇÃO

Proposta de Recomendações para a Aplicação das Práticas e Processos do ITIL na Gestão de Riscos de SOA - Arquitetura Orientada a Serviços

Diogo Gomes Silva

Welerson Fernandes Lopes

Brasília, Dezembro de 2013

UNIVERSIDADE DE BRASILIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA

Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

Proposta de Recomendações para a Aplicação das Práticas e Processos do ITIL na Gestão de Riscos de SOA - Arquitetura Orientada a Serviços

Diogo Gomes Silva

Welerson Fernandes Lopes

Relatório submetido como requisito parcial para obtenção
do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Dr. Edgard Costa Oliveira (Orientador)
Universidade de Brasília

Prof. Dr. Rafael Timóteo de Sousa Jr
Universidade de Brasília

Prof. Dr. Flávio Elias de Deus
Universidade de Brasília

Dedicatória(s)

Dedico este trabalho primeiramente a Deus por ter me proporcionado os meios de concluir meu curso de graduação, aos meus pais, irmã e namorada por terem compreendido minhas ausências durante este período de minha vida acadêmica, aos irmãos que na UnB tive pelo apoio e força nos momentos difíceis.

Diogo Gomes Silva

Dedico este trabalho em especial a Deus por permitir e fornecer meios que possibilitassem minha evolução enquanto estudante de graduação, aos meus pais, aos meus irmãos e a minha namorada pelo apoio e consideração em minha caminhada durante a graduação.

Welerson Fernandes Lopes

Agradecimentos

Agradeço aos professores que na UnB transmitiram parte de seus conhecimentos e me proporcionaram desenvolver habilidades necessárias a minha formação. Ao professor Edgard pela paciência, cordialidade e boa vontade na orientação deste trabalho.

Diogo Gomes Silva

Agradeço aos professores, que durante minha formação na UnB, contribuíram de forma significativa para minha evolução enquanto profissional e pessoa. Ao professor Edgard pela paciência, cordialidade e boa vontade na orientação deste trabalho. Ao meu melhor amigo e parceiro de projeto final por partilhar dos momentos difíceis e felizes ao longos destes anos na graduação.

Welerson Fernandes Lopes

“A mente que se abre a uma nova ideia jamais volta ao seu tamanho original.”

Albert Einstein

RESUMO

O presente trabalho apresenta conceitos básicos acerca de ITIL, SOA e gestão de segurança da informação. Devido à versatilidade da tecnologia SOA seus conceitos e princípios têm se difundido, ao mesmo passo em que riscos e situações de insucesso têm sido observados, muitas vezes levando a fracasso na implantação SOA. A literatura aponta que na maioria dos casos de fracasso SOA, a falta de governança adequada foi a responsável. No trabalho são apresentados riscos associados a SOA obtidos por meio de pesquisa bibliográfica. Por fim, como contribuição do trabalho, propomos recomendações baseadas em ITIL para gestão de riscos de SOA.

ABSTRACT

This work presents basic concepts about ITIL, SOA and information security management. Due to the versatility of SOA tecnology, their concepts and principles have been spread at the same time in which risks and situations of failure have been observed, often leading to failure in implementing SOA. The literature shows that in most cases of SOA failure, lack of proper governance was responsible. Are presented risks associated with SOA obtained by means of literature at work. Finally, as a contribution of the this work we propose recommendations based on ITIL to risk management for SOA

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

Siglas

ABNT	Associação Brasileira de Normas Técnicas
CCTA	*Central Computer and Telecommunications*
COBIT	*Control Objectives for Information and related Technology*
EAI	*Enterprise Application Integration*
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ITIL	*Information Technology Infrastructure Library*
PMBOK	*Project Management Body of Knowledge*
SI	Sistema de Informação
SLA	*Service Level Agreement*
SOA	Arquitetura Orientada a Serviços
TI	*Tecnologia da Informação*

1Introdução

Este capítulo apresenta as considerações preliminares acerca do projeto, no que diz respeito ao problema a ser solucionado, os objetivos, geral e específicos assim como a metodologia a ser utilizada.

1.1 O problema

SOA (Arquitetura Orientada a Serviços) é um paradigma de desenvolvimento de sistemas baseado em computação distribuída que proporciona alto nível de abstração, desenvolvimento e execução de sistemas distribuídos, encobrindo uma série de detalhes no que diz respeito à plataforma. Flexibilidade e reuso, tanto de lógica quanto de hardware, têm tornado SOA como um dos paradigmas de desenvolvimento em ascensão no mercado. Junto a tal ascensão constata-se o aparecimento de vulnerabilidades, bem como a busca destas por indivíduos mal intencionados. Questões inerentes a SOA, como abertura e autonomia de serviço, trazem consigo riscos aos sistemas (LOWIS, 2011).

A governança SOA faz parte da governança de TI. ITIL por sua vez é um dos guias de gestão de TI mais adotados mundialmente, trazendo as melhores práticas de serviços de TI, com um framework que pode ser adaptado para uso em todos os negócios e ambientes organizacionais (CLINCH, 2009). Logo ITIL pode trazer maior eficiência e efetividade para a gestão de segurança da informação em SOA.

À medida que a tecnologia da informação é aplicada nos mais diversos setores, encontramos sistemas em que questões de segurança da informação são tão importantes quanto à própria funcionalidade da aplicação, sistemas críticos onde a mínima falha em qualquer aspecto do sistema não é tolerável, assim como acontece em um sistema de bancário (ARRAJ, 2010).

Devido à possibilidade de uso e evolução de sistema legado, reuso de serviços, flexibilidade e independência de plataforma utilizada, SOA tem se tornado um dos paradigmas de desenvolvimento de sistemas mais aceitos e utilizados, principalmente em sistemas de grande porte, como práticas adotadas em diversos segmentos de mercado e áreas do governo.

Na adoção de SOA, muitas organizações se deparam com desafios significativos, sendo que somente uma porção dessas organizações conseguiu maximizar lucros. Os problemas em geral foram atribuídos à falta de planejamento para desenvolvimento de serviço, falta de estratégia de longo prazo, progresso lento no desenvolvimento, falta de padrões uniformes para o desenvolvimento de serviço, ausência de plano de emergência para tratar exceções e resposta lenta à mudança de serviços (XIAN-PENG, BI-YING e RUI-FANG, 2012).

Pesquisas mostram que as principais causas de falha em SOA são originadas de falta de governança SOA e não de aspectos tecnológicos propriamente ditos (CLINCH, 2009).

Vemos que juntamente com o crescente uso de SOA surge a necessidade de busca e eliminação de vulnerabilidades de forma a tornar eficiente, e com o devido propósito, a transição e execução de um sistema para SOA.

Tendo em vista buscar meios para tornar o projeto, implementação e operação de SOA mais eficiente, buscamos com nosso trabalho propor recomendações baseadas em ITIL para a Gestão de Riscos de SOA - Arquitetura Orientada a Serviços.

1.2 Objetivos

1.2.1 Objetivo geral

Propor um conjunto de recomendações baseadas na biblioteca ITIL para a Gestão de Riscos de SOA - Arquitetura Orientada a Serviços.

1.2.2 Objetivos específicos

a. Pesquisa e apresentação de conceitos referentes a ITIL, SOA e gestão de segurança da informação;

b. Pesquisa e identificação dos riscos associados a Arquitetura Orientada a Serviços - SOA;

c. Elaborar propostas de recomendações de segurança baseadas em ITIL para a gestão de riscos de SOA.

1.3 Metodologia

Para atingir os objetivos do trabalho os seguintes procedimentos foram utilizados, para cada um dos objetivos específicos;

Objetivo a: Pesquisa e apresentação de conceitos referentes a ITIL, SOA e segurança da informação:

- levantamento de pesquisa bibliográfica;
- análise documental.

Objetivo b: Pesquisa e identificação dos riscos associados à Arquitetura Orientada a Serviços -SOA

- pesquisa bibliográfica;
- análise documental;
- levantamento de riscos de SOA;

Objetivo c: Elaborar propostas de recomendações de segurança baseadas em ITIL para a gestão da segurança de SOA.

- pesquisa bibliográfica;
- análise documental;
- mapeamento dos riscos SOA aos processos de ITIL, por meio de tabela;
- Busca das recomendações na biblioteca ITIL para os riscos mapeados.

2 Revisão de literatura

Este capítulo consta dos conceitos teóricos que serão abordados ao longo de todo o escopo do trabalho.

2.1 A biblioteca ITIL

No final da década de 80 a CCTA (*Central Computer and Telecommunications Agency*), órgão ligado ao governo da Inglaterra, construiu um banco com informações de diversas organizações e empresas sobre processos relacionados à área de TIC (Tecnologia da Informação e Comunicações). Este banco de informações resultou em um livro de orientações, que, apesar de ter sido criado para ser implantado no governo, foi visto com bons olhos pelas empresas privadas que perceberam a aplicabilidade destas soluções para seus negócios. O resultado deste processo foi a compilação de um compêndio (biblioteca) com orientações de melhores processos e melhores práticas de gestão de serviços em TI, tendo como característica a independência de plataforma e tecnologia. Este documento passou a ser conhecido com ITIL - *Information Technology Infrastructure Library*.

A ITIL é um modelo público e livre, ou seja, seu uso não gera custos autorais e que vem sempre sendo atualizada através da expertise de profissionais da área de TI. A atual versão da ITIL é a 3.0, instituída em 2007 e atualizada recentemente em 2011.

2.1.1 Conceitos de ITIL

Serviços são definidos pela ITIL como um valor entregue à empresa que vise obter resultados com o melhor custo benefício, diminuindo riscos associados. Para agregar valor aos serviços é necessário que ele preencha o requisito de utilidade, ou seja, o serviço tem de estar adequado às necessidades do cliente, e ao requisito de garantia, no qual o serviço deve estar disponível quando necessário para o uso. O gerenciamento destes serviços é a capacidades de fornecer valor final aos clientes na forma de serviços.

2.1.2 ITIL como ferramenta corporativa

Sabe-se hoje que a informação é o mais importante ativo e recurso estratégico que uma organização precisa gerenciar. Desta forma é de suma importância reconhecer que os serviços de TI ocupam uma posição decisiva nas empresas, sendo necessário investir e gerir níveis adequados de recursos de TI.

As organizações de TI precisam ser continuamente capazes de majorar objetivos anteriormente previstos aos seus serviços de forma mais eficiente possível, pois o ambiente de negócios é de certa forma volúvel e a ITIL traz esta flexibilidade exigida, através de um modelo de melhoria continua de serviço.

Embora as tecnologias de hoje nos permitam ser capazes de fornecer recursos robustos e oferecerem flexibilidade significativa, elas são muito complexas. O alcance global disponível para as empresas através da Internet oferece grande oportunidade de negócios ao apresentar desafios adicionais em relação à confidencialidade, integridade e disponibilidade de serviços e dados. Além disso, as organizações de TI precisam continuar a ser capazes de atender ou exceder as expectativas de serviço durante o trabalho da forma mais eficiente possível. Processos repetitivos e consistentes são a chave para a eficiência, a eficácia e a capacidade de melhorar os serviços. Estes processos repetitivos consistentes são descritos no modelo ITIL (ARRAJ, 2010).

2.1.3 Ciclos de vida

São cinco as fases do ciclo de vida que constituem ITIL, sendo cada fase focada em um objetivo, conforme figura 2.1;

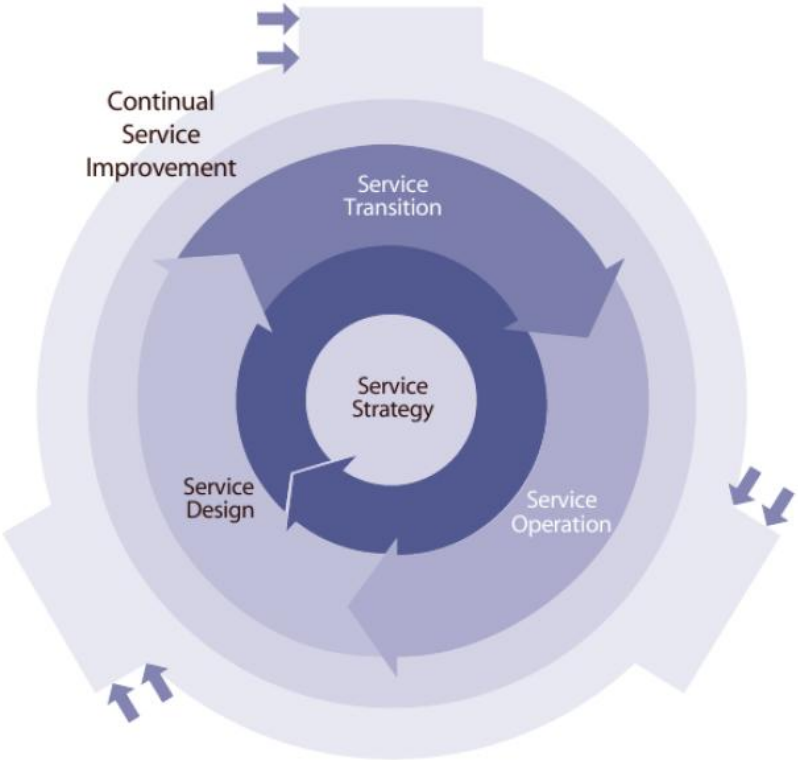

Figura 2.1- Ciclos de vida ITIL v3 (ITILv3 OFFICIAL INTRODUCTION, 2007)

2.1.3.1 Fase 1: Estratégia do serviço (Service Strategy)

A Estratégia de Serviço é o ponto de partida do ciclo de vida de um serviço na ITIL v3 provendo orientações de como desenhar, desenvolver e implementar o gerenciamento de serviços não somente como uma habilidade organizacional, mas sim como um ativo estratégico. Nesta fase, são providas orientações sobre os princípios que sustentam o gerenciamento de serviços que são úteis no desenvolvimento de políticas de gerenciamento de serviços, recomendações e processos em todo o ciclo de vida de serviço da ITIL (ITIL, SERVICE STRATEGY, 2007).

Processos da fase:
- Gerenciamento de portfólio de serviço;
- Gerenciamento da demanda;
- Gerenciamento financeiro de TI.

2.1.3.2 Fase 2: Desenho de Serviço (Service Design)

O Desenho de Serviço é segunda fase do ciclo de vida do ITIL, fornece os princípios e métodos de desenho para converter os objetivos estratégicos em portfólios e ativos de serviços, garantindo que os serviços de TI estão alinhados às necessidades de negócio. Tem como objetivo principal a concepção de serviços de TI em conformidade com as práticas, processos e políticas de governança de TI para consolidar a estratégia e facilitar a introdução destes serviços no ambiente de produção e desta forma assegurar a qualidade da entrega dos serviços, a satisfação dos clientes e o custo-benefício na prestação dos serviços (ITIL, SERVICE DESIGN, 2007).

Processos da fase:
- Gerenciamento do catálogo de serviço;
- Gerenciamento de nível de serviço;
- Gerenciamento da capacidade;
- Gerenciamento da disponibilidade;
- Gerenciamento da continuidade do serviço de TI;
- Gerenciamento da segurança da informação;
- Gerenciamento de fornecedor.

2.1.3.3 Fase 3: Transição do serviço (Service Transition)

A Transição de Serviço fornece orientações para o desenvolvimento e melhoria da capacidade de transição de serviços novos e modificados. Mostra como os requisitos da Estratégia de Serviço codificados no Desenho de Serviço serão realizados na Operação de Serviço, controlando os riscos de falhas e interrupções. Em linhas gerais, ela serve como um elo que liga a fase de Desenho de Serviço à fase de Operação de Serviço (ITIL, SERVICE TRANSITION, 2007).

Processos da fase:
- Planejamento e suporte da transição;
- Gerenciamento da configuração e ativo de serviço;
- Gerenciamento de liberação e implantação;
- Teste e validação de serviço;
- Avaliação;
- Gerenciamento de mudança;
- Gerenciamento do conhecimento.

2.1.3.4 Fase 4: Operação do serviço (Service Operation)

A Operação de Serviço incorpora práticas para o gerenciamento dos serviços em operação. Ela fornece diretrizes para adquirir eficácia e eficiência na entrega e suporte dos serviços, assegurando a entrega de valor ao cliente e ao provedor de serviço. Além de, proporcionar orientações para manter a estabilidade dos serviços em operação, permitindo realização de mudanças no projeto, escopo e níveis de serviços acordos (ITIL, SERVICE OPERATION, 2007).

Na Operação de Serviço, é possível gerenciar as aplicações, as tecnologias e a infraestrutura que suportam os serviços, permitindo aos gestores tomarem decisões melhores a respeito do gerenciamento da disponibilidade dos serviços, do controle de demanda, da otimização da utilização da capacidade, do escalonamento das operações e até mesmo corrigir problemas (ITIL, SERVICE OPERATION, 2007).

Processos da fase:

- Gerenciamento de eventos;
- Gerenciamento de incidentes;
- Cumprimento de requisição;
- Gerenciamento de problemas;
- Gerenciamento de acesso.

2.1.3.5 Fase 5: Melhoria contínua do serviço (Continual Service Improvement)

A Melhoria de Serviço Continuada é fundamental na criação e manutenção de valor para os clientes. Combinando os princípios, práticas e métodos de gestão de qualidade, gestão de mudanças e melhoria da capacidade ela permite as organizações realizarem melhorias incrementais e em grande escala na qualidade dos serviços, eficiência operacional e continuidade do negócio (ITIL, CONTINUAL SERVICE IMPROVEMENT, 2007).

As atividades de Melhoria de Serviço Continuada são executadas durante todo o ciclo de vida, atuando na integração e melhoria de todas as fases e possibilitando o realinhamento dos serviços de TI para atender às mudanças nas necessidades do negócio (ITIL, CONTINUAL SERVICE IMPROVEMENT, 2007).

2.2 SOA – Arquitetura Orientada a Serviços

SOA é uma abordagem para integração de arquiteturas baseadas no conceito de serviço, pois é uma tecnologia que aplica conceitos que foram utilizados com sucesso em implementações de desenvolvimento orientado a objetos, desenho baseado em componentes e tecnologias de EAI – *Enterprise Application Integration*, Integração de aplicações corporativas. (KEEN, 2004)

Para Müller (2009) SOA é um conjunto de princípios e melhores práticas para implementação e execução de processos de negócio automatizados em ambientes de TI heterogêneos.

Segundo Erl (2009) uma implementação de SOA pode consistir em uma combinação de tecnologias, produtos, API's, extensões da infraestrutura de suporte e várias outras partes. A implementação da arquitetura orientada a serviços, em cada empresa, é exclusiva; contudo,

ela é caracterizada pela introdução de novas tecnologias e plataformas que suportam especificamente a criação, a execução e a evolução das soluções orientadas a serviços.

Bieberstein apresenta SOA como uma forma de aproximar a linguagem do negócio à linguagem da TI. Para ele, o conceito de serviço é um caminho natural para compreender a empresa e o negócio. "SOA não é tecnologia, SOA é negócio". (BIEBERSTEIN, 2008)

High afirma que "o objetivo principal de SOA é alinhar o mundo dos negócios com o mundo da TI, tornando ambos mais efetivos". (HIGH, KINDER e GRAHAM, 2005).

Professores da UnB envolvidos no projeto RES, o qual utiliza SOA, afirmam que, "Atualmente SOA é a melhor opção disponível para alcançar as metas de agilidade, interoperabilidade e reutilização que são comuns a muitas organizações". (ALCANTARA, *et al*).

"Arquitetura Orientada a Serviços (SOA) é um poderoso paradigma de computação distribuída, que proporciona alto nível de abstração para desenvolvimento, implementação, e execução de sistemas distribuídos, enquanto esconde muitos detalhes de plataforma". (GRONOSKY e ATIGHETCHI, 2010).

Vemos então que SOA é um padrão de tecnologia que representa uma evolução, ao longo da história da TI, de todos os aspectos satisfatórios, ligando-os aos negócios.

SOA estabelece um paradigma de projeto que visa aprimorar a eficiência, agilidade e produtividade de uma empresa, colocando os serviços como o principal meio para que as soluções lógicas sejam representadas no suporte aos objetivos estratégicos associados à computação distribuída, ao mesmo tempo em que abstrai vários detalhes de tecnologia, fazendo com que diversas abordagens e plataformas diferentes possam interagir (GRONOSKY, ATICHGETCHI e PAL, 2010).

Por meio da leitura de um pouco da literatura SOA é possível perceber que SOA não pode ser reduzido a mero produto de software. Muito mais que isso, SOA é um paradigma de projeto que guia todos os aspectos de criação e uso de serviços de negócio através de todo o ciclo de vida de desenvolvimento (desde a fase de concepção até a aposentadoria de serviços), bem como trata da definição e do provisionamento da infraestrutura de TI, permitindo que diferentes aplicações troquem dados e participem de processos de negócios, independentemente dos sistemas operacionais ou linguagens de programação utilizadas para sua implementação. (NEWCOMER e LOMOW, 2005).

Os serviços são os artefatos centrais de SOA, os ativos primários de arquitetura. Juntamente com os serviços deve ser definido um modelo de projeto de serviços que assegure reutilização, interoperabilidade e integração por todos os processos de negócio e plataforma de tecnologias.

A tecnologia é essencial para apoiar e alcançar SOA, mas a iniciativa SOA não se resume a uma tecnologia. A tecnologia deve ser disponibilizada para permitir que os serviços operem de forma confiável e segura, apoiando os objetivos do negócio e permitindo evoluir na arquitetura de TI existente, possibilitando, por exemplo, que sistemas legados possam ser utilizados em processos de negócio a fim de apoiar os objetivos de SOA. Em muitas organizações sistemas legados são os principais componentes envolvidos em serviços SOA (BHALLAMUDI e TILLEY).

Um dos maiores desafios de SOA é que ele não é implementado de uma só vez. Ao invés disso, ele é alcançado através de muitos projetos distintos ao longo do tempo e em diferentes localizações (ou departamentos). Essa distribuição temporal e espacial dos projetos de SOA faz da governança o fator mais crítico para o sucesso de SOA. A governança e as políticas de execução são as chaves para a gestão de conformidade de SOA pelos horizontes de tempo e espaço (BHALLAMUDI e TILLEY).

Diversos autores defendem que SOA não surgiu do nada e também não é um paradigma de projeto revolucionário, apenas que este é uma representação da evolução de TI, constituindo-se de paradigmas, boas práticas e tecnologias do passado. Por tanto SOA não pretende substituir tudo que o precedeu, ao contrário disso, aproveita-se do passado e o combina com modelagens e princípios para tirar o maior proveito de inovações tecnológicas recentes (HAFNER e BREU, 2009).

A fim de desenvolver e implementar serviços em uma arquitetura SOA, é necessário a utilização de uma metodologia eficaz para análise, especificação, desenvolvimento e governança de serviços. Essa metodologia deve permitir aos interessados tirar o maior proveito deste novo tipo de abordagem, diminuindo os riscos inerentes ao projeto. Todavia, SOA não pode ser comprado a partir de uma prateleira ou adquirido da internet, SOA é uma jornada. Como visto SOA não é tecnologia nova, pois o uso de TI para direcionar os objetivos do negócio vem desde os primórdios da computação.

2.2.1- Princípios do paradigma SOA

A seguir são apresentados os princípios nos quais um sistema SOA se baseia. Para esta seção tomamos como base os princípios apresentados por Thomas ERL, 2009, em seu livro: SOA, Princípios de Design de Serviços. Thomas Erl possui várias publicações a respeito de SOA, e tem reconhecimento internacional acerca do tema.

2.2.1.1-Contrato de serviço padronizado

O contrato de serviço formaliza e documenta consistentemente as capacidades e propósitos que um serviço deverá ter, surgindo devido à necessidade de interconexão entre componentes independentes e autônomos do sistema. Tal contrato estabelece os termos de compromisso, fornecendo restrições e requisitos técnicos, bem como toda informação sobre a semântica que o proprietário do serviço desejar publicar.

Considerado um dos princípios mais importantes em SOA, o contrato de serviço explicita a interface do serviço, ditando quais dados serão trocados entre os mesmo e quais os formatos serão utilizados por estes dados. O contrato é, portanto, a interação de um serviço com os demais serviços autônomos e independentes.

Com a programação orientada a serviços, a noção de reuso de componentes é levada à tona (princípio herdado da modelagem orientada a objetos). É justamente na fase de elaboração do contrato de serviço que deve-se dar maior ênfase à ideia de reuso, pois é nessa fase em que definimos o quão genérica será a interface do serviço. Quanto mais genérica possível, maior a possibilidade de reuso futuro, e por tanto, mais bem estabelecido o contrato se tornará (ERL, 2009).

2.2.1.2-Baixo acoplamento de serviço

Um acoplamento entre serviços refere-se à interconexão entre os mesmos. A forma como esses irão trocar dados de modo ao resultado de um serviço servir de entrada para outro. A idéia do princípio SOA de baixo acoplamento entre serviços está diretamente ligada à independência e autonomia que o serviço terá. Quanto menor for um acoplamento, menos determinado serviço, em tempo de execução, dependerá de resultados de um outro serviço, tornando-o um serviço com maior capacidade de reuso. Uma medida do nível de acoplamento entre serviços está relacionada ao nível de dependência entre os mesmos. Tal dependência sempre irá existir uma vez que um serviço depende o resultado de outro para poder executar sua funcionalidade, logo o acoplamento é inevitável, porém buscamos minimizá-lo.

Promovendo consistentemente um fraco acoplamento entre os serviços tendemos a aumentar sua independência, promovendo um ambiente SOA em que um serviço e seus consumidores podem se evoluir ao longo do tempo, com impacto mínimo de um serviço sobre os demais serviços que dependem dele. Promovendo o baixo acoplamento, colocamos o serviço como um recurso constantemente disponível, e evitamos que o relacionamento deste com demais não iniba evolução futura dos mesmos.

Em um sistema SOA podemos observar uma serie de diferentes acoplamentos, como:

- Acoplamento de lógica ao contrato;
- Acoplamento de contrato à lógica;
- Acoplamento de contrato à tecnologia;
- Acoplamento de contrato à implementação;
- Acoplamento de contrato à funcionalidade.

O objetivo do princípio de baixo acoplamento é diminuir todas essas formas de acoplamento com exceção do acoplamento entre contrato e lógica, já que este é o relacionamento entre o contrato e o que será desempenhado pelo serviços, logo estes devem ter alto acoplamento (ERL, 2009).

2.2.1.3-Abstração de serviço

A noção de abstração de serviço consiste em ocultar informações do serviço que não são necessárias para a utilização deste por demais serviços consumidores. Devido à orientação a serviços tratar dos serviços como produtos comerciais independentes, a abstração durante a fase de projeto de um serviço se torna de essencial importância. Quanto mais informações forem entregues para consumidores, maior será a percepção de plataformas, soluções e detalhes proprietários do serviço, o que pode ser indesejável no mundo do comércio. Aumenta-se também a possibilidade de maior acoplamento, já que o consumidor terá mais amarras ao contrato. Logo este princípio visa manter no contrato uma quantidade de informação concisa e equilibrada, evitando também o acesso a informações desnecessárias que dizem respeito ao contrato de serviço. Este princípio requer investimento em tempo para avaliação de valor e risco ao que será publicado a respeito um serviço. A abstração pode ser aplicada aos seguintes campos;

- Informações tecnológicas;
- Informações funcionais;
- Informações lógicas programáticas;
- Qualidade de informações de serviço (variedade de informações e detalhes do serviço).

A fim de se avaliar o nível de abstração devemos levar em consideração o contrato de serviço, pois determinada área, das listadas acima, pode ter parte de abstração limitada por requisitos de contrato (ERL, 2009).

2.2.1.4-Capacidade de reuso de serviço

Trata-se de um dos objetivos mais fundamentais para se alcançar o propósito da arquitetura orientada a serviços (SOA). Segundo Thomas ERL (2009), os outros princípios SOA existem para dar suporte a este. O conceito de reuso consiste em tornar o serviço útil para mais de um propósito, podendo sua funcionalidade ser reaproveitada em diferentes sistemas.

Para tornar um serviço o mais reusável possível, devemos levar em conta todos os diversos cenários nos quais o mesmo poderá ser inserido, de forma a tentar otimizar e tornar o mais genérica possível a sua lógica. Tal otimização nunca será tão efetiva, quanto à observada em softwares de propósito único, projetado com uma única finalidade. O reuso pode nos levar a perder a liberdade de evoluções arbitrárias na funcionalidade e mesmo lógica do serviço, uma vez que este pode estar sendo reusado nos mais diferentes cenários, alterações podem afetar o uso por parte dos consumidores. O objetivo primordial de SOA é utilizar de seus princípios para lidar com estes problemas. Desde a concepção de um serviço o mesmo deve ser pensando com base em reuso.

O reuso aumenta complexidade, tempo, custos e esforços para se produzir software, porém caso atinja um nível considerável de reuso poderá trazer retorno muito alto frente ao investimento inicial para desenvolvimento do serviço.

Para Thomas ERL (2009): ”*Quando vemos o serviço como um ativo de TI que exige investimento, mas tem potencial de retornos repetidos, é possível avaliar por que temos que ter cuidado ao projetar cada parte da arquitetura de um serviço*”.

2.2.1.5-Autonomia de serviço

A autonomia de serviço diz respeito à capacidade de se auto governar, dizendo respeito a um software que é capaz de executar sua lógica independentemente de influências externas. Aumentar a autonomia de serviço significa limitar a dependência que o serviço tem de componentes externos (outros serviços). Tal aumento de autonomia proporciona maior confiança e previsibilidade em relação à operação do serviço uma vez que este terá maior grau de controle sobre seus recursos (ERL, 2009).

Temos dois diferentes tipos de autonomia na implementação de serviços:

- Autonomia em tempo de execução;

  Proporciona maior controle sobre confiabilidade, desempenho, previsibilidade e requisitos de segurança da funcionalidade do serviço.

- Autonomia na Etapa de *design;*

  Diz respeito à fidelidade que o serviço tem com o contrato, logo os requisitos podem ficar amarrados já nesta etapa, de tal forma que impedirá modificações futuras no serviço, perdendo o proprietário do serviço a autonomia na etapa de *design*, uma vez que serviços consumidores já estão vinculados a este.

2.2.1.6-Visibilidade do serviço

O princípio da visibilidade em SOA é o que proporciona o meio para se fazer a descoberta de serviços em SOA. É devido a esse principio que podemos saber se determinada funcionalidade que é preciso para uma solução já existe, ou se devemos cria-la, logo precisamos de informações sobre os recursos já disponíveis. As informações tidas como essenciais são: propósito, capacidade e limitações de capacidade do serviço. Neste princípio vemos que além de produzir um serviço o mais genérico possível a fim de se aproveitar dos benefícios do reuso, devemos também produzir boa informação sobre o mesmo, a fim de que a visibilidade do serviço atinja seu propósito, e não haja a possibilidade de se criar serviços com funcionalidade redundante só pelo simples fato de a descoberta do mesmo não ser eficiente (ERL, 2009).

Propósitos e capacidades do serviço devem ser claramente expressos a fim de que a capacidade de reuso SOA seja atingida.

2.2.1.7-Composição de serviços

A composição de serviços permite que a capacidade ou propósito de um serviço seja combinado com a de outros, para a solução de um problema maior. Boa parte da capacidade de reuso em SOA é realizada por meio da composição de serviços (ERL, 2009).

2.2.1.8- Independência de estado de serviço

Na composição de serviços, podem surgir situações nas quais um serviço tenha que, em tempo de processamento, esperar pelo resultado da funcionalidade de outro serviço. Determinados serviços devem processar e reter, em um banco de dados, suas informações enquanto esperam pelo processamento de outro serviço. Tal fato pode exaurir recursos do sistema, principalmente porque várias instâncias do serviço podem estar rodando em uma

mesma plataforma. O princípio da Independência de Estado de Serviço surge para evitar que cenários como este surjam, tendo a finalidade de maximizar a escalabilidade, e tirar o máximo proveito de qualquer limite que desempenho que o sistema esteja sujeito. De acordo com o princípio da independência de estado, o serviço deve ser projetado de forma a depender o mínimo possível de tempo do estado que um outro serviço na composição se encontre.

De acordo com a lógica de uma composição será impossível fazer com que determinado serviço não dependa da informação de estado de outro. De forma a minimizar o impacto nessas situações, soluções como o diferimento e delegação de informação de estado foram criadas. Tais soluções consistem em se delegar a responsabilidade de manter informações de estado a outra parte da arquitetura do sistema, a exemplo de um banco de dados. Assim outros serviços podem consultar o mesmo, e a disponibilidade do serviço que delegou a função seria aumentada (ERL, 2009).

2.3 Fundamentos de segurança da informação

Cada vez mais as organizações têm de lidar com grande quantidade de modificações nos negócios, e se adaptar a diferentes ambientes, com o propósito de garantir competitividade. Tais modificações trazem novos requisitos de segurança. Para incorporar os novos requisitos, a gestão de riscos e segurança da informação se faz necessária. "Com a segurança correta, os objetivos de negócio são atingidos e suas finalidades garantidas, mesmo quando ocorrerem influências negativas internas ou externas, ou se a infraestrutura de TI falhar" (OVERBEEK, CAZEMIER e PETERS, 2009).

Incidentes em segurança não são predominantemente causados por falhas técnicas, pois estatísticas mostram que a maioria deles é ocasionada por falhas humanas, intencionais ou não (CLINCH, 2009).

LOWIS (2011) define segurança da informação como: "*A Soma de todas as técnicas, métodos, procedimentos e atividades empregadas, para manter um estado específico ideal, por meio de um conjunto de regras que dizem o que é autorizado e o que não é sem sistemas de informação heterogêneo, descentralizado, e interconectado*".

O Gestor de segurança da informação deve entender que segurança não é uma etapa do ciclo de via de serviços e sistemas, e que segurança não pode ser resolvida por meio de tecnologias. Ao invés disso, segurança da informação deve constituir uma parte integrante de todos os serviços e sistemas, e que deve ser um processo continuamente gerenciado, usando um conjunto de controles de segurança (ITIL, SEVICE DESIGN, 2007).

O objetivo da Gestão de Segurança da Informação é alinhar a segurança da informação, incluído a segurança de TI (tecnologias), com os requisitos de segurança de negócio, garantindo que a segurança da informação será efetivamente administrada.

As organizações estão cada vez mais dependentes de serviços de TI para atingir seus objetivos de negócios, logo estão também cada vez mais dependentes de uma boa gestão de informação. Nesse contexto, "Segurança da Informação não é um objetivo por si só, muito além disso, é uma garantia de se atingir os objetivos de negócio" (OVERBEEK, CAZEMIER e PETERS, 2009).

A Segurança da Informação têm três princípios tidos como pilares para se considerar um ambiente seguro, são eles:

- Confidencialidade;
- Integridade;
- Disponibilidade.

A confidencialidade diz respeito a termos certeza com quem ou o que estamos nos conectando e trocando informações, dentro ou fora da organização. A Integridade por sua vez é o principio que nos garante que as informações não serão modificadas em seu repositório ou transito, podendo então se confiar nas mesmas. Por fim a Disponibilidade é a garantia de que o sistema estará pronto para uso sempre que precisarmos. Tais princípios devem ser tidos como condições normais na operação de negócios. Uma organização deve, portanto, organizar seu repositório, manipulação e processamento de informação de tal forma que essas condições sejam satisfeitas (OVERBEEK, CAZEMIER e PETERS, 2009).

Manter uma infraestrutura de TI segura custa dinheiro, devido a recursos, manutenção e controle. Não manter a infraestrutura de TI segura, também custa dinheiro, na perda de produção, equipamentos danificados, dados corrompidos ou interceptados. O pior no aspecto da abordagem de não manter a segurança seria que no caso de uma falha, a reputação da empresa poderia se abalar de forma irreversível.

Riscos são aspectos inevitáveis da vida de negócio, e devem ser geridos. Tanto riscos conhecidos como os desconhecidos devem ser administrados. "*Esteja preparado para o inesperado*" (OVERBEEK, CAZEMIER e PETERS, 2009).

2.3.1- Princípios para sistemas seguros

Nesta seção listamos os princípios apontados por Paul OVERBEEK (2009), sobre os quais um projetista de sistemas deve se embasar a fim de que o ambiente busque a segurança da informação:

- **Isolamento:** componentes críticos devem ser isolados, a fim de que seja mais fácil o controle de seu comportamento e diagnostico;
- **Padrão a prova de falhas:** o sistema deve negar tudo o que não seja explicitamente autorizado, a fim de que se previna vulnerabilidades causadas por omissão ou negligência;
- **Uso de arquiteturas abertas:** a segurança não depende de uma arquitetura secreta, procure utilizar arquiteturas conhecidas, pois essas são excessivamente testadas, e uma arquitetura secreta, não o será para sempre.
- **Controle de privilégios:** utilize controle de privilégios a fim de que as responsabilidades no sistema seja bem delimitada, restringido acessos ao diferentes setores.
- **Funcionalidades limitadas:** limite as funcionalidades a que um usuário terá acesso, permitindo que o mesmo só utilize o que for necessário para sua função, dessa forma vulnerabilidades são limitadas;
- **Ergonomia:** a interface do sistema de ser projetada de tal forma que minimize a possibilidade de erros e permitir a detecção dos mesmos, a fim de se evitar erros acidentais;
- **Redundância:** evitar que um sistema tenha uma única base de acesso, a fim de que a disponibilidade não esteja prejudicada na falta desta. Podemos ter redundância no controle de acesso, armazenamento, *host* de um sistema, etc.
- **Adaptabilidade:** flexibilidade para que o mecanismo de segurança possa ser trocado no futuro, pois os requisitos podem mudar, ou mesmo tal mecanismo pode não ser mais seguro.
- **Mecanismos de resiliência:** Os servidos devem ter mecanismos para mostrar quando estão em mau funcionamento e se possível corrigir automaticamente a falha ou vulnerabilidade;
- **Avisos:** o sistema deve providenciar informações sobre seu próprio funcionamento e eventos definidos.
- **Autenticação:** validação e aceitação à entrada no sistema.
- **Controle de Acesso:** permitir acesso à informação ou funções no sistema apenas a pessoas autorizadas.

2.4 - Gestão de segurança da informação

A informação é um ativo essencial para os negócios de uma empresa e consequentemente necessita ser protegido, ainda mais nos ambientes de negócio cada vez mais interconectados, fato que fez com a informação ficasse mais exposta a grande variedade de ameaças e vulnerabilidades.

A norma ISO NBR 27002 define segurança da informação como a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar riscos, maximizar retorno sobre os investimentos e aumentar oportunidades de negócio. (ABNT NBR ISO/IEC 27002, 2005).

Para a ITIL a gestão de segurança da informação é definida como: ”*O processo que garante Confidencialidade, Integridade e Disponibilidade para os ativos de uma organização, informação, dados e serviços de TI. Gestão de Segurança da Informação geralmente é parte da tentativa de uma empresa em implementar a Gestão de Segurança, a qual tem um escopo mais amplo do que serviços de TI.* ” (ITIL, OFFICIAL INTRODUCTION, 2007).

Michel Faber (2010) define risco como um evento incerto ou um conjunto de eventos, que caso acorra terá um efeito na conquista de objetivos. Um risco consiste na combinação de probabilidade de uma ameaça ocorrer e a magnitude de seu impacto nos objetivos de negócio.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware.* Estes controles precisam ser estabelecidos, implementados, monitorados, analisados e melhorados, para garantir que os objetivos do negócio e de segurança sejam atendidos. Neste cenário surge a gestão de segurança da informação (ABNT NBR ISO/IEC 27002, 2005).

Gestão de Segurança da Informação é essencialmente uma série de atividades que mantém um nível específico de segurança da informação e TI. A Gestão de Segurança da Informação lida com o estabelecimento e manutenção de tudo que é preciso para manter o nível de segurança da informação necessário. Levando em conta os riscos externos ou mesmo mudanças nos processos de negócio. O nível necessário de segurança deve ser estabelecido para manter o risco de negócios em um nível acordado e aceitável (OVERBEEK, CAZEMIER e PETERS, 2009).

Como atingir o nível necessário de segurança da informação é atribuição da gestão de segurança da informação, que o faz por meio de análise de riscos, definição de medidas de controle apropriados, criar padrões, implementar e monitorar operações.

A gestão de segurança da informação é um processo de esforço contínuo, verificando-se a efetividade da segurança no dia-a-dia da operação do sistema, e comparando-se essa efetividade com os requisitos estabelecidos.

2.4.1- Norma ISO ABNT 27002

A NBR ISO/IEC 27002 é um código de boas práticas para a gestão da segurança da informação, mantido por comitê internacional da ISO/IEC. Tem como finalidade prover diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação em uma organização. A norma pode ser usada por uma organização como um guia prático para desenvolver procedimentos e estabelecer práticas de gestão da segurança da informação (ABNT ISO/IEC 27002).

A NBR ISO/IEC 27002 é formada por 11 seções de controles de segurança da informação, os quais são divididas em categorias principais de segurança, que totalizam 39 categorias (ABNT ISO/IEC 27002).

Abaixo veremos os objetivos e escopo das seções de controle que formam a norma ISO/IEC 27002.

2.4.1.1- Análise e avaliação de riscos

As análises e avaliações de riscos precisam identificar e priorizar os riscos com base nos critérios para aceitação dos riscos e dos objetivos relevantes para a organização. Os resultados obtidos vão orientar e determinar as ações de gestão que serão apropriadas para o gerenciamento de riscos de segurança da informação (ABNT ISO/IEC 27002).

A análise e avaliação dos riscos precisa ter seu escopo bem definido para ser eficiente e produzir o efeito desejado. Devendo estimar a magnitude do risco e comparar os riscos estimados com os critérios para determinar a significância dos riscos. Todo esse processo precisa ser realizado regularmente para cobrir as mudanças nos requisitos de segurança e situações de riscos(ABNT ISO/IEC 27002).

2.4.1.2- Política de segurança da informação

A política de segurança da informação desempenha um papel importante para o planejamento estratégico da segurança da informação, pois é por meio dela que se fornece

orientação e apoio à segurança da informação de acordo com os requisitos do negócio, leis e regulamentações pertinentes.

O documento da política de segurança da informação deve ser acessível, compreensível, declarar o comprometimento da direção e o enfoque da organização no gerenciamento da segurança da informação. Este documento deve ser aprovado pela direção, publicado e comunicado a todos os funcionários e partes externas relevantes (ABNT ISO/IEC 27002).

Na análise da política de segurança da informação deve-se considerar os seguintes aspectos: situações de ações preventivas e corretivas, resultado de análises anteriores, desempenho do processo e conformidade com a política de segurança da informação, mudanças no ambiente organizacional, tendências de ameaças e vulnerabilidades, relato sobre incidentes de segurança e recomendações de autoridades relevantes.

Como resultado da análise espera-se obter: melhora dos controles e seus objetivos, melhor alocação de recursos e responsabilidades, assim como do alinhamento da segurança da informação com os objetivos do negócio (ABNT ISO/IEC 27002).

2.4.1.3- Organizando a segurança da informação

Esta seção da norma tem por objetivo o gerenciamento da segurança da informação dentro da organização. Estabelece que uma estrutura de gerenciamento seja criada para iniciar e controlar a implementação de segurança da informação dentro da organização. Se necessário deve ser disponibilizada consultoria especializada em segurança da informação. Contatos com especialistas ou grupos de segurança da informação externos, autoridades relevantes, devem ser feitos para se manter atualizado com as tendências de mercado.

A coordenação da segurança da informação tem de garantir que as atividades de segurança sejam executadas de acordo com sua política, para isso deve identificar os descumprimentos à norma, identificar possíveis ameaças, avaliar e implementar controles, assim como as informações de monitoramento e de análise dos incidentes de segurança, promover a educação, treinamento e conscientização por toda a organização.

Para organizar a segurança da informação é necessário que as responsabilidades de segurança estejam definidas claramente e em conformidade com a política de segurança. Para isso, primeiramente, é necessária a identificação dos ativos e processos de segurança da informação de cada área, para então designar os seus responsáveis. Após a escolha dos gestores de cada área, deve-se definir suas atribuições e os detalhes deste processo devem ser inteiramente documentados.

2.4.1.4- Gestão de ativos

A gestão de ativos tem como objetivo alcançar e manter a proteção dos ativos da organização, que são definidos pela norma como sendo qualquer coisa que tenha valor para a organização. Por exemplo, informações, softwares, hardwares, serviços, pessoas e suas qualificações, a reputação e a imagem da organização.

A norma estabelece que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido. Devem ser identificadas, documentadas e implementadas regras para que sejam permitidos o uso de informações e de ativos associados aos recursos de processamento da informação.

Informações devem ser classificadas e rotuladas em termos de seu valor, requisitos legais, sensibilidade e criticidade para a organização com o objetivo de receberem um nível adequado de proteção.

2.4.1.5- Segurança em recursos humanos

A segurança de recursos humanos tem por objetivo assegurar que os funcionários, fornecedores e terceiros estão conscientes das ameaças e preocupações relativas à segurança da informação, suas responsabilidades e obrigações, e estão preparados para apoiar a política de segurança da informação da organização durante os seus trabalhos normais, e para reduzir o risco de erro humano. Responsabilidades individuais devem ser definidas para garantir que a segurança da informação seja aplicada em todo trabalho individual dentro da organização.

Um nível adequado de conscientização, educação e treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação seja fornecido para todos os funcionários, fornecedores e terceiros, para minimizar possíveis riscos de segurança da informação. Um processo formal para tratar das violações de segurança da informação deve ser estabelecido.

2.4.1.6- Segurança física do ambiente

Áreas seguras devem ser estabelecidas tendo em vista a prevenção de acesso físico não autorizado, danos e interferências com as instalações e informações da organização. Instalações de processamento da informação críticas ou sensíveis devem ser mantidas em áreas seguras, protegidas por perímetros de segurança definidos, com barreiras de segurança e controles de acesso apropriados.

Equipamentos devem ser levando em consideração na segurança do ambiente com o objetivo de impedir perdas, danos, furtos ou roubos, comprometimento de ativos e interrupção das atividades da organização.

2.4.1.7- Gerenciamento de operações e comunicações

O gerenciamento de operações e comunicações tem por objetivo garantir a operação segura e correta dos recursos de processamento da informação. Devem ser definidos os procedimentos e responsabilidades pela gestão e operação de todos os recursos de processamento das informações, abrangendo o desenvolvimento de procedimentos operacionais apropriados. A segregação de funções é apropriada, para reduzir o risco de mau uso ou uso doloso dos sistemas.

Os procedimentos de operação devem ser documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem. Modificações nos recursos de processamento da informação e sistemas devem ser controladas. Recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

2.4.1.8- Controle de acesso

O controle de acesso tem o objetivo de controlar o acesso à informação. O acesso a informação, recursos de processamento das informações e processos de negócios devem ser controlados com base nos requisitos de negócio e segurança da informação. As regras de controle devem levar em consideração as políticas para autorização e disseminação da informação.

O gerenciamento de acesso do usuário deve assegurar acesso de usuário autorizado e prevenir acesso não autorizado a sistemas de informação. A distribuição de direitos de acesso deve ser controlada, dando especial atenção a direitos de acesso privilegiados onde os usuários são permitidos a mudar controles de sistemas.

Políticas de responsabilidades dos usuários devem ser estabelecidas, com o objetivo de prevenir acesso não autorizado dos usuários e evitar o comprometimento ou furto de informações e recursos de processamento da informação. A cooperação de usuários autorizado é essencial para uma efetiva segurança. Usuários devem estar conscientes de suas responsabilidades para manter efetivo controle de acesso, particularmente em relação ao uso de senhas e de segurança dos equipamentos de usuários.

O controle de acesso à rede tem o objetivo de prevenir acesso não autorizado aos serviços de rede. Acesso aos serviços internos e externos de rede devem ser controlados. Os usuários de serviços não podem comprometer a segurança, assegurando-se autenticação e controle de acesso.

2.4.1.9- Aquisição, desenvolvimento e manutenção de S.I.

Os requisitos de segurança da informação tem o objetivo de garantir que segurança seja parte integrante de sistemas de informação. Sistemas de informação incluem sistemas operacionais, infra-estrutura, aplicações de negócios, produtos de prateleira, serviços e aplicações desenvolvidas pelo usuário. O projeto e a implementação de sistemas de informação destinados a apoiar o processo de negócios podem ser cruciais para a segurança. Os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento de sistemas de informação.

O processamento correto nas aplicações tem o objetivo de prevenir a ocorrência de erros, perdas, modificação não autorizada ou mau uso de informações em aplicações. Controles apropriados devem ser incorporados no projeto de aplicações, inclusive aquelas desenvolvidas pelos usuários, para assegurar o processamento correto. Controles adicionais podem ser necessários para sistemas que processem informações sensíveis, valiosas ou críticas, ou que nestas exerçam algum impacto.

2.4.1.10- Gestão de incidentes de segurança da informação

A notificação de fragilidade e eventos de segurança da informação tem o objetivo de assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a ação corretiva em tempo hábil. Procedimentos formais de registro e escalonamento devem ser estabelecidos. Todos os funcionários, fornecedores e terceiros devem estar conscientes sobre os procedimentos para notificação dos diferentes tipos de eventos e fragilidades que possam ter impactos na segurança dos ativos da organização. Inconformidades devem ser informadas tão logo quanto o possível.

A gestão de incidentes de segurança da informação e melhorias tem o objetivo de assegurar que um enfoque consistente e efetivo seja aplicado à gestão de incidentes de segurança da informação. Um processo de melhoria contínua deve ser aplicado às respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.

2.4.1.11- Gestão de continuidade do negócio

A gestão de continuidade do negócio tem o objetivo de não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso. Processo de gestão de continuidade deve ser implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação a um nível aceitável através da combinação de ações de prevenção e recuperação. Controles devem ser implementados para identificar e reduzir riscos, limitando as consequências aos danos do incidente e garantindo que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

2.4.1.12- Conformidade

A conformidade com requisitos legais tem o objetivo de evitar que violações de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais, e de quaisquer requisitos de segurança da informação. Convém que consultoria em requisitos legais específicos seja procurada em organizações de consultoria jurídica ou em profissionais liberais, adequadamente qualificados nos aspectos legais.

3 Riscos associados a SOA

Este capítulo apresenta alguns riscos inerentes aos princípios de SOA. Os riscos apresentados tratam-se de riscos a serem resolvidos em um nível gerencial.

3.1 Introdução

Independentemente da tecnologia de informação utilizada, SOA só poderá ser utilizada de forma satisfatória caso leve em consideração princípios da segurança da informação. Dependendo da situação a segurança do sistema é tão importante quanto sua funcionalidade. Com o uso crescente o paradigma de desenvolvimento de sistemas SOA, aumenta-se a preocupação com segurança de sistemas que utilizam tal tecnologia, assim como aumenta-se a motivação de pessoas mal intencionadas em encontrar vulnerabilidades no mesmo (GHAFAR, SALEH e MODIRI, 2011).

Considerando-se aspectos de segurança em uma migração para SOA, são observados casos que demonstraram sérias falhas. Fatores como tecnologia utilizada, forma de migração, sistema legado e governança SOA estão entre os mais observados nos cenários de falha. Pesquisas realizadas pela revista TechTarget/Forrester "Research State of SOA" em 2010 mostram que 65% das soluções SOA implementadas foram tidas como sucesso por seus responsáveis (23,19 % tiveram sucesso considerável, 42,39% apresentaram algum sucesso), os restantes 35% dos projetos SOA apresentaram falhas em sua implementação.(BHALLAMUDI e TILLEY)

Além de más práticas na implementação SOA, esta tecnologia traz consigo algumas vulnerabilidades inerentes ao seu uso, como por exemplo a reutilização de serviços. Um serviço que seja implementado com falha poderia estar sendo utilizado em diversos processos de diferentes aplicações, logo a mesma falha ou vulnerabilidade poderia ser explorada em diferentes sistemas. (HOJAJI, SHIRAZI e AYATOLLAZADEH)

Uma das formas de desenvolver uma plataforma segura para SOA é conhecer as fraquezas e vulnerabilidades inerentes à mesma. Não podemos simplesmente utilizar técnicas de segurança de software, como criptografia para tornar SOA seguro, devemos no entanto nos preocupar com a construção de uma plataforma segura, conhecendo e desde a base mitigando fraquezas e vulnerabilidades (MACGRAW, 2006).

É visto então que os desafios em relação à gestão de segurança da informação crescem à medida que migramos para SOA, uma vez que esta tecnologia expõe suas vulnerabilidades mais expressivamente do que observado em tecnologias anteriores.

3.2 Riscos em SOA

Listaremos agora os riscos inerentes a SOA associados a cada um dos princípios, vistos na revisão bibliográfica. Tomamos como base os riscos apresentados por Thomas ERL (2009) em seu livro, SOA princípios de design de serviços. Trata-se de um conjunto de riscos a serem considerados a um nível gerencial (alto nível), portanto julgamos pertinente buscar mitigar tais riscos com a elaboração de propostas de recomendações baseadas na biblioteca ITIL.

3.2.1 Riscos associados ao contrato de serviço

Controle de versão

Os contratos de serviços podem ter a necessidade de evoluir com o passar do tempo, como por exemplo, determinado formato de dado pode não ter sido bem planejado, e no futuro resultar em problemas graves para a execução em determinado contexto do sistema. O problema dessa evolução está no fato de que várias dependências deste serviço podem ter sido criadas por consumidores do mesmo devido ao reuso (quanto mais reusável a lógica do serviço mais dependências são criadas), existindo forte acoplamento do serviço com os demais. Mudança nos requisitos irão exigir modificações na implementação do serviço, podendo até mesmo violar o contrato de serviço o que irá exigir novas versões do mesmo, existindo então a necessidade de controle dessas versões.

Dependências de tecnologia

Para implementar um serviço SOA podemos escolher entre diferentes linguagens de programação e plataformas de desenvolvimento, tanto em tecnologias abertas como em proprietárias. O risco associado à tecnologia que um serviço foi implementado está no fato que essas possuem níveis de maturidade e tempo de vida. Uma plataforma de tecnologia nova e aprimorada pode surgir, tornando a plataforma na qual determinado serviço foi implementado obsoleta. Logo, como o contrato de serviço é o único ponto de entrada para a funcionalidade encapsulada pelo serviço o uso dessa tecnologia pode se tornar inviável.

3.2.2 Riscos associados ao baixo acoplamento

Problemas de desempenho

Na tentativa de reduzir a dependência entre serviços, podemos criar esquemas de contratos excessivamente simplificados, ficando um serviço genérico ao ponto de não ter funcionalidade. Um alto nível de flexibilidade pode trazer também uma necessidade de maior processamento por parte do serviço, uma vez que este teria que desprender de parte da lógica apenas para fazer interpretação de dados. Logo os requisitos de desempenho do serviço aumentam à medida que levamos o acoplamento a um nível mais baixo.

3.2.3 Riscos associados à abstração de serviço

Requisitos de acoplamento de múltiplos consumidores

Consumidores de serviços têm necessidades diferentes, logo pode acontecer de determinado nível de abstração ser adequado a um consumidor, porém ser insuficiente para atender a requisitos de outro. Dessa forma a abstração influencia de forma direta a aplicabilidade e reuso de um serviço. Uma avaliação descabida do nível de abstração pode limitar a capacidade do consumidor de usar um serviço, trazendo insucesso ao mesmo.

Interpretação errada pelas pessoas devido ao excesso de abstração

Na tecnologia SOA, o contrato de serviço é o que explicita os propósitos, capacidades e requisitos de serviços. Como o princípio da abstração resulta na ocultação deliberada de informação, uma abstração exagerada pode fazer com que o contrato traga informações insuficientes para que o usuário julgue um serviço útil, o que pode levar a intepretações erradas a respeito funcionalidades do mesmo. Insatisfação por parte do consumidor e perda de possibilidade de reuso, mesmo que o serviço tenha bons propósitos e qualidade.

3.2.4 Riscos associados à capacidade de reuso de serviço

Preocupações com governança

Uma vez que grande quantidade dos serviços são reutilizáveis, as abordagens tradicionais de governança não são mais aplicáveis, uma vez que pequenos grupos externos à empresa irá cada um ter controle de seu próprio módulo (serviço), estando a própria organização com um controle pequeno sobre o processo. Tal fato pode prejudicar a evolução do sistema, já que os serviços são produzidos de forma independentes, e o *designer* pode estar preocupado apenas com as necessidades de sua própria solução, não pensando no todo.

Preocupações com disponibilidade

Um serviço reutilizado com sucesso pode trazer o problema de disponibilidade para várias empresas, já que um único ponto de serviço pode representar um ponto de falha para vários e diferentes processos. Caso um serviço deixe de estar disponível por qualquer motivo (exemplo de indisponibilidade no host que o hospeda), todos os consumidores que dependem do mesmo deixaram de funcionar.

Preocupações com segurança

Um serviço criado sem levar em consideração os aspectos de segurança da informação pode, por meio do reuso, proliferar suas vulnerabilidades por uma serie de processos consumidores do mesmo. "*Reuso de um serviço vulnerável permite aos indivíduos mal intencionados a reutilizar estratégias de ataque*" (LOWIS e ACCOSI, 2011).

Preocupações com desenvolvimento ágil

A produção de serviços com alta capacidade de reuso, demanda de tempo e dinheiro. Análises detalhadas de diferentes cenários devem ser feitas, a fim de que o sucesso seja obtido. A preocupação com todos esses aspectos pode acabar demandando bastante de recursos para desenvolvimento do projeto. Logo, empresas em que o desenvolvimento ágil é o princípio de negócio terão problemas em produzir software reusável. Organizações que trabalham com serviços ágeis pensam em retorno do investimento de longo prazo. A agilidade na entrega de soluções só é atingida a partir do momento que quantidade considerável de software reusável já estiver disponível, sendo o trabalho do projetista agora apenas realizar

chamadas a estes. Porém este é um nível em que SOA terá atingido sua maturidade, o que exige esforço e investimento prévio.

3.2.5 Riscos associados à visibilidade do serviço

Aplicar o princípio da visibilidade após a implementação do serviço

O risco aqui está no fato da perda de detalhes da funcionalidade do serviço por esquecimento, uma vez que o princípio está sendo aplicado somente depois de o serviço já ter sido implantado. O ideal é que desde o início da etapa de implementação do serviço já exista preocupação referente à visibilidade do serviço por parte dos consumidores. Os próprios desenvolvedores do serviço têm os detalhes minuciosos do mesmo, logo estes seriam os mais indicados para fazerem o esboço do princípio de visibilidade concomitantemente com a implementação do serviço.

Utilizar linguagem de difícil interpretação

Não devemos supor que consumidores de serviço tenham o mesmo grau de perícia técnica daqueles que o implementaram. Os serviços devem ser descobertos e interpretados por diversos profissionais de TI. A dificuldade de interpretação do contrato de serviço por parte de usuários poderia comprometer o reuso de um serviço com bons propósitos e funcionalidades.

3.2.6 Riscos associados à composição de serviços

Serviço membro de composição como único ponto de falha em cascata

O risco aqui está no fato de que um único serviço que tiver sua disponibilidade prejudicada pode afetar toda a composição. Um serviço pode ser membro de várias composições ao mesmo tempo, logo todas essas poderiam ser afetadas no caso de falha neste serviço.

Membros de composição como gargalo de desempenho

O tempo de resposta de cada membro da composição deve ser levado em consideração, uma vez que um único serviço membro pode afetar o desempenho total da composição.

3.2.7 Riscos associados à independência de estado de serviço

Exigência de maior desempenho em tempo de serviço

As soluções de independência de estado que envolvem a delegação por outro membro da guarda da informação de estado, como um banco de dados, aumentam a disponibilidade do serviço, porém exige um maior esforço de processamento uma vez que o mesmo demandará de maior poder de processamento para atualizar, manter, processar e interpretar informações de estado que teria que buscar no banco de dados.

4 Proposta para o uso de ITIL na gestão de riscos de SOA

Este capítulo apresenta a nossa contribuição para o trabalho, onde buscamos mapear cada um dos riscos apresentados por SOA a cada um dos processos de ITIL e assim buscar as recomendações dadas por este.

4.1 Introdução

O uso de TI hoje tem se tornado essencial para os negócios. Porém, ter simplesmente a melhor tecnologia não irá garantir benefício na utilização da mesma. Profissionalismo, responsabilidade e boa gestão é o que proporciona a qualidade do serviço nos negócios (ITIL, OFICIAL INTRODUCTION, 2007).

Governança é definida por Susanti, como o uso intencional de políticas, planos, procedimentos e estruturas organizacionais para tomada de decisões e controlar uma entidade de forma a atingir seus objetivos de negócio (SUSANTI e SEMBIRING, 2011).

Governança em um contexto geral diz respeito à tomada de decisões e o caminho no qual os processos são implementados. Quando se trabalha com governança, estamos envolvidos na análise de processos, e no sistema no qual a organização trabalha (FABER e FABER, 2010).

É prática costumeira na academia e no mercado o aprendizado com os erros, evitamos que os mesmos aconteçam novamente e aperfeiçoamos nossas boas práticas. ITIL teve seu escopo definido ao longo dos anos através de experiências vividas por grandes empresas na área de TI, por isso se torna um código de boas práticas de excelência.

SOA é uma tecnologia de TI que tem se tornado popular, ao passo que problemas em sua implementação tem se tornado mais sérios. Dessa forma a governança SOA tem sido tema bastante discutido, de forma a se ter um guia de como planejar, implementar e operar SOA para que este maximize os objetivos.

Muitas organizações têm apresentado *frameworks* com soluções para governança SOA, porém muitas têm se mostrado insuficientemente alinhada às necessidades de SOA, ficando alguns processos sem cobertura. Com este propósito tanto Xian-Peng , Bi-ying e Rui Fang (2012), quanto Susanti e Sembiring (2011) de forma independente escreveram artigos onde propuseram de forma satisfatória uma solução para a governança SOA tendo como base todo o

ciclo de vida ITIL, definindo cada uma das fases, e processos dentro dessas, por meio dos processos definidos em ITIL.

A governança SOA faz parte da governança de TI, e os métodos usados por ITIL para resolver problemas está de acordo com a teoria de governança SOA. O conceito de ciclo de vida é também apropriado para a gestão de governança SOA (XIAN-PENG, BI-YIUNG e RUI-FANG, 2012).

Baseado no mapeamento, a governança SOA tem conexão com ITIL v3, especialmente em processos, e elementos que suportam o reuso de serviços (SUSANTI e SEMBIRING, 2011).

Os artigos citados mostraram que ITIL é aplicável de forma satisfatória à governança SOA. Queremos então com nosso trabalho nos concentrar aos riscos apresentados na implantação e operação de SOA e buscar recomendações para a gestão de riscos na biblioteca ITIL para mitiga-los.

4.2 Aplicação de ITIL na gestão de segurança

Em ITIL a gestão de segurança da informação é definida como: ”O processo que garante Confidencialidade, Integridade e Disponibilidade para os ativos de uma organização, informação, dados e serviços de TI. Gestão de Segurança da Informação geralmente é parte da tentativa de uma empresa em implementar a Gestão de Segurança, a qual tem um escopo mais amplo do que serviços de TI. ” (ITIL, OFFICIAL INTRODUCTION, 2007).

Ao longo dos anos as organizações estão ficando cada vez mais dependentes de Tecnologia da Informação para atingir seus objetivos de negócio. Tal perspectiva tem resultado em uma crescente demanda de serviços de TI. A Disponibilidade de serviços tem se tornado um aspecto decisivo na competitividade de uma empresa que tem TI como negócio, uma vez que a satisfação do consumidor de serviços de TI está diretamente ligada à disponibilidade do serviço para seu uso. “*Disponibilidade de serviço tem um impacto dramático na satisfação do consumidor e na reputação da empresa, uma vez que os consumidores estão a um só clique no mouse de migrar para o concorrente*” (ZENG, 2008).

“*Muito esforço e desenvolvimento têm sido feito para garantir alta disponibilidade em cada tecnologia*”. Os riscos para a disponibilidade de serviços são causados por cada uma das partes envolvidas nos sistemas de TI, desde a tecnologia, até falhas humanas. “*Não existe pesquisa e foco o suficiente para entender e melhorar a disponibilidade de serviço de TI fim-a-fim da perspectiva do usuário*“ (ZENG, 2008).

Existe grande tendência na preocupação com questões puramente técnicas, porém estatísticas mostram que os erros humanos estão na raiz de mais da metade das falhas de aspecto de segurança em serviço de TI, enquanto questões técnicas causam menos de um décimo das falhas. Medidas técnicas são importantes, porém uma visão mais ampla se faz necessária (CLINCH, 2009).

Vemos ao longo da literatura que uma boa gestão de serviços de TI é primordial para atingir tanto a disponibilidade suficiente para o sucesso do serviço, quanto para lidar com os cenários de falha que possam surgir. ITIL define um *framework* que ajuda as empresas de TI definirem uma estrutura organizacional e conhecimentos necessários. Trás também um conjunto de procedimentos padrões de gestão, que possibilita as organizações a aplicar a gestão nos processos de TI e infraestrutura associada. Os procedimentos são independentes de plataforma e aplicáveis a todos os aspectos de Tecnologia da Informação. "*ITIL especificamente alinha o valor da estratégia de negócio de TI com a necessidade da entrega de serviços de alta qualidade*" (ZENG, 2008).

4.3 Alinhamento entre os riscos associados a SOA e os processos dos ciclos de vida da ITIL

Nesta seção mapearemos cada um dos riscos apresentados na seção 3.3 com os processos dos ciclos de vida da ITIL vistos na revisão bibliográfica, e em seguida buscaremos as recomendações para cada um nos livros da ITIL. O Mapeamento apresentado na **Tabela 4.1** foi feito com base na análise do escopo de cada processo dos ciclos de vida da ITIL.

Tabela 4.1- Mapeamento entre os riscos associados a SOA e os processos de ITIL

Riscos apresentados por SOA	**Etapa do Clico de Vida da ITIL**	**Processos da ITIL**
Controle de Versão	Desenho de Serviço / Transição de Serviço	Gerenciamento de Catálogo de Serviço/ Gerenciamento de Configurações e de Ativos de Serviço
Dependências de tecnologia	Desenho de Serviço	Gerenciamento de Capacidade
Problemas de desempenho	Desenho de Serviço/ Estratégia de Serviço	Gerenciamento de Capacidade/ Gerenciamento de Demanda

Tabela 4.1 – Mapeamento entre os riscos associados a SOA e os processos de ITIL		
Riscos apresentados por SOA	**Etapa do Clico de Vida da ITIL**	**Processos da ITIL**
Requisitos de acoplamento de múltiplos consumidores	Desenho de Serviço	Gerenciamento de Nível de Serviço
Interpretação errada pelas pessoas devido a excesso de abstração de serviço	Desenho de Serviço	Gerenciamento de Catálogo de Serviço
Preocupação com governança	Todos	Todos
Preocupação com disponibilidade	Desenho de Serviço/ Operação de Serviço	Gerenciamento de Disponibilidade/ Gerenciamento de Incidente
Preocupação com segurança	Desenho de Serviço	Gerenciamento de Segurança da Informação
Preocupação com desenvolvimento ágil	Transição de Serviço	Planejamento e Suporte da Transição
Aplicar o princípio da visibilidade após a implementação do serviço	Desenho de Serviço/ Estratégia de Serviço	Gerenciamento de Catálogo de Serviço/ Gerenciamento de Portfólio de Serviço
Não utilizar linguagem de fácil interpretação no contrato de serviço	Desenho de Serviço	Gerenciamento de Catálogo de Serviço
Serviço membro de composição como único ponto de falha em cascata	Desenho de Serviço	Gerenciamento de Disponibilidade/ Gerenciamento de Continuidade do Serviço de TI
Membros de composição como gargalo de desempenho	Desenho de Serviço / Estratégia de Serviço	Gerenciamento de Capacidade/ Gerenciamento de Demanda
Exigência de maior desempenho em tempo de serviço	Desenho de Serviço / Estratégia de Serviço	Gerenciamento de Capacidade / Gerenciamento de Demanda

4.3.1 Risco 1: Controle de versão

Foi visto ao longo do nosso trabalho que os requisitos na implementação e operação dos serviços sofrem modificações com o passar do tempo. Como visto na seção 3.2.1 tais modificações nos requisitos podem até mesmo violar o contrato de serviço, exigindo novas

versões do mesmo. O problema surge quando não é feito um controle eficiente destas diferentes versões.

Buscamos em ITIL uma forma de tornar mais eficiente o controle de versão dos serviços SOA. Após analisado o escopo dos processos ITIL, mapeamos este risco nos processos de Gerenciamento de Catálogo de Serviço, do ciclo de vida Desenho de Serviço e de Gerenciamento de Configurações e de Ativos de Serviço.

A proposta do processo de Gerenciamento de Catalogo de Serviço é providenciar uma única fonte consistente de informação sobre todos os serviços, e garantir que a mesma seja amplamente disponível para aqueles que tenham permissão de acesso. O Catálogo de Serviço deve conter todos os detalhes de todos os serviços atualmente em uso. (ITIL, SERVICE DESIGN, 2007).

O Gerenciamento de Configurações e de Ativos de Serviço por sua vez tem o objetivo de identificar, controlar, guardar, auditar, e verificar itens de ativos de serviço e de configurações, incluindo versões, componentes constituintes suas atribuições e relacionamentos. (ITIL, SERVICE TRANSITION, 2007).

Vemos que pelas propostas do processo de Gerenciamento de Configurações e de Ativos de Serviço, o mesmo busca criar e manter um inventário consistente de ativos de Serviço, propiciando a devida identificação de cada um. O Gerenciamento de Catálogo de Serviço por sua vez traz informações detalhadas a cerca de cada item desse inventário.

Gerenciando-se melhor o fornecimento de informações sobre os serviços como um todo, melhora-se o controle sobre versão dos mesmos, uma vez que novos requisitos e especificações serão melhor detalhados.

Processos Propostos por ITIL

- Definição do Serviço;
- Produção e manutenção de um Catálogo de Serviço consistente;
- Interfaces, dependências e consistência entre Catálogo de Serviço e Portfólio de Serviço;
- Interfaces e dependências entre todos os serviços, componentes suporte e itens de configuração;

Atividades Propostas por ITIL

- Acordos e documentação da definição do serviço entre todas as partes relevantes;
- Interfaceamento do Gerenciamento de Portfólio de Serviço com o Gerenciamento de Catálogo de Serviço;

- Produzir e manter o Catálogo de Serviço e seus recursos, em conjunto com o Portfólio de Serviço;
- Interfacemanto com grupos de suporte, fornecedores e Gerenciamento de Configuração, para acordo de Catálogo de Serviço Técnico;
- Interfaceamento com Gerenciamento de Relações de Negócios e Gerenciamento de Nível de Serviço para garantir que as informações estejam alinhadas com os negócios e processos de negócios.

4.3.1.1 Recomendações para o risco de controle de versão

A fim de se gerenciar o controle de versão de serviços SOA deve-se produzir um catálogo de serviços consistente e documentado. Para se produzir tal catálogo trazendo o nível de detalhamento que proporcione a correta interpretação das funcionalidades, e requisitos das diferentes versões do serviço, deve-se buscar o auxílio de grupos de suporte, fornecedores, assim como periodicamente se proceder com pesquisas aos usuários dos serviços, buscando compreender como os mesmos conseguem enxergar o serviço, apenas por meio da interpretação da documentação do mesmo. Garantimos dessa forma que o nível de informações transmitidas aos potenciais consumidores do serviço sejam suficientes para que os mesmos possam fazer a escolha certa quando estiverem procurando por um serviço.

4.3.1.2 Crítica à recomendação

O maior desafio com o gerenciamento de catálogo de serviços está em se manter um catálogo de serviços conciso e incorporar tal prática no dia a dia dos negócios, uma vez que a cultura da empresa pode julgar tal atividade desnecessária. Para se tirar benefícios do catálogo de serviços, a empresa deve primeiramente estabelecer a cultura de que o catálogo e o portfólio de serviço são fontes essenciais de informação que todos os envolvidos na área de TI da organização deve utilizar e ajudar a manter. Manter um controle rigoroso no catálogo de serviços exige que uma equipe de trabalho, ferramentas e recursos sejam mantidos somente para tal finalidade. Tal aspecto pode demandar de bastante investimento financeiro e de tempo o que pode ser dispendioso para empresas de pequeno porte.

4.3.2 Risco 2 : Dependências de tecnologia

Foi visto ao longo do deste trabalho que SOA pode implementar serviços utilizando diferentes linguagens de programação e plataformas de desenvolvimento. O risco inerente à dependência tecnológica está no fato de que uma determinada tecnologia em que um serviço foi implementado, pode ter se tornado obsoleta, a ponto de impossibilitar seu uso, prejudicando os sistemas, serviços ou composições que necessitavam daquela funcionalidade.

Após análise do escopo dos processos ITIL o risco de dependência de tecnologia para SOA foi mapeado no processo de Gerenciamento de Capacidade ITIL. Tal processo deve levar em consideração todas as áreas tecnológicas, tanto em *hardware* quanto *software*, para os componentes e ambientes de TI.

Uma das atividades da Gestão de Capacidades é lidar com o conhecimento do potencial para a entrega de novos serviços. Novas tecnologias devem ser consideradas, e se apropriado, usadas para inovar e entregar os serviços necessários aos clientes. Deve-se levar em consideração o crescimento da taxa de mudanças na tecnologia, e que deve se tirar proveito dessas evoluções para garantir a continuidade da satisfação dos negócios (ITIL, SERVICE DESIGN, 2007).

A gestão de Capacidade deve ter ligação direta com a Estratégia de Serviço e Portfólio de Serviço, para garantir que tecnologias emergentes sejam consideradas nos planejamentos de serviço futuro.

O processo de Gestão de Capacidade deve ser responsável por verificar mudanças nos requisitos para novas demandas dos consumidores, dando suporte a novos serviços ou mesmo modificações nestes. Pode-se requerer modificações na tecnologia legada para dar suporte às funcionalidades extras.

Processos e Técnicas Propostas por ITIL

- Verificar tendências na utilização dos atuais componentes do sistema e estimar os requisitos futuros, a partir dessas informações estabelecer metas para o planejamento de inovação e melhorias;
- Modelar e buscar a implementação das modificações previstas para serviços de TI, identificar as mudanças que precisam ser feitas nos serviços, componentes da infraestrutura e aplicações de TI, garantindo que os recursos necessários estarão disponíveis;
- Garantir que as melhorias serão avaliadas, planejadas e testadas antes que acordos de nível de serviço (SLA’s) ou problemas na performance do sistema ocorram.

Atividades Propostas por ITIL

- Exploração de novas tecnologias, a qual envolve o conhecimento de novas técnicas e tecnologias, assim como o conhecimento de como essas podem ser utilizadas para dar suporte ao negócio. Informações como essas podem ser adquiridas por meio da:
    - Literatura profissional, como revistas e artigos;
    - Promoção de seminários com fornecedores de *hardware* e *software;*
    - Participação em reuniões entre fornecedores potenciais de *hardware* e *software;*
    - Reunião entre profissionais usuários envolvidos na gestão de capacidade de empresas.

Cada uma dessas atividades providencia informações relacionadas às técnicas, tecnologia, hardware e software que serão vantajosas para implementar e adquirir os benefícios de negócio.

4.3.2.1 Recomendações para o risco de dependências de tecnologia

A fim de que um fornecedor de serviços SOA não corra o risco de ter a operação de algum serviço inviabilizada por dependência de tecnologia, o mesmo deve verificar tendências e realizar testes na operação dos atuais componentes do sistema. Requisitos futuros devem também ser estimados, para assim se fazer o correto planejamento de sistemas novos. Para se proceder com tal verificação e análise do cenário, de forma a estimar as necessidades, o fornecedor se serviços SOA deve sempre buscar a atualização de seus conhecimentos a respeito da tecnologia, buscando informações em literatura profissional e participando de reuniões, congressos, conferências, onde concentrará potenciais fornecedores e parceiros de negócio, e o tema em questão será discutido.

4.3.2.2 Crítica à recomendação

Podemos verificar que a exploração de novas tecnologias pode ser inviável em cenários onde as soluções devem ser imediatas, onde não se dispõe do tempo necessário para a pesquisa detalhada. Sendo possível essa consideração apenas nos ambientes de longo prazo. O aspecto de investimento financeiro deve também ser lavado em consideração, pois mesmo que se saiba que uma determinada tecnologia seria mais benéfica, uma organização poderia não dispor dos recursos necessários para adoção da mesma.

4.3.3 Risco 3 : Problemas de desempenho

Como visto na seção 3.2.2, um alto nível de flexibilidade no serviço pode fazer com o mesmo demande de maior capacidade de processamento, uma vez que utilizará maior parte da sua lógica apenas para interpretação de dados, aumentando assim os requisitos de desempenho.

Devemos dimensionar os recursos de forma a termos uma melhor relação custo-benefício. Com base no escopo dos processos ITIL foi feito o mapeamento deste risco em dois processos diferentes, são eles: Gerenciamento de Capacidade, dentro do ciclo de vida Desenho de Serviço, e Gerenciamento de Demanda, dentro do ciclo de vida Estratégia de Serviço ITIL.

O grande desafio em lidar com a Gestão de Capacidade está em entender o relacionamento entre demanda e requisitos do negócio, e traduzir essa relação em termos de avaliação de impactos e efeitos na utilização dos serviços (ITIL, SEVICE DESIGN, 2007).

A Gestão de Capacidade deve ser o ponto focal quando se busca a performance e capacidade dos recursos de TI, tanto no que diz respeito a recursos de *hardware* e *software* quanto a recursos humanos, já que limitações nestes também podem fazer com que tarefas não sejam cumpridas com o devido desempenho.

Alinhado com a Gestão de Capacidade deve estar a Gestão de Demanda uma vez que esta deverá dimensionar qual o nível de capacidade coerente para o sistema. Não devemos ter falta de capacidade para prover serviços, como também não se deve ter excesso, para que recursos não sejam desperdiçados.

A Interface entre os processos de Gestão de Capacidade e Gestão de Demanda ITIL permite garantir que recursos de TI sejam planejados e implementados de forma a providenciar um nível consistente de serviço que garanta as necessidades de desempenho atuais e futuras.

Fazer a gestão de capacidade de infraestruturas distribuídas de TI é uma atividade dispendiosa e complexa, especialmente quando a capacidade está ligada a investimentos financeiros. Porém o crescimento de tal infraestrutura pode ser planejado de forma ao seu custo não comprometer os recursos da empresa. Podemos fazer tal planejamento dessa forma:

- Em quais componentes será necessário o *upgrade* (exemplo: mais memória, dispositivos de armazenamento mais rápidos, processadores mais rápidos, maior largura de banda), quando será necessário o *upgrade*;
- Quando fazer o *upgrade;*
- Quanto o *upgrade* irá custar;

Processos e Técnicas Propostas por ITIL

- Antever questões de desempenho, tomando as ações necessárias antes que problemas ocorram;
- Verificar tendências na utilização dos componentes atualmente em funcionamento e estimar os requisitos futuros, usando limiares para planejar evoluções;
- Modelar previamente as mudanças nos serviços de TI, avaliando pontos críticos na infraestrutura e nas aplicações, garantindo o desempenho do serviço;
- Sempre que financeiramente justificável buscar o aumento do desempenho do serviço;
- Otimizar o desempenho de serviços e componentes;
- Monitorar, medir, produzir dados e rever o desempenho corrente de serviços e componentes;

Atividades Propostas por ITIL

- Monitoramento do Serviço: É importante que os dispositivos de monitoramento coletem todos os dados necessários para o processo de Gestão de Capacidade, dados típicos monitorados são:
    - Utilização do Processador;
    - Utilização de Memória;
    - Utilização de Dispositivos;
    - Tamanho de Filas;
    - Utilização de Disco;
    - Tempo de Resposta;
    - Uso de Dados;
    - Taxa de Conflitos;
    - Numero de Usuários no Sistema;
    - Taxa de Tráfego na Rede.

  Sistemas de alarme são importantes para quanto algum dos dados coletados estiverem próximo do valor limite estabelecido.
- Análise: Os dados coletados no monitoramento devem ser analisados de forma a se verificar tendências na utilização do serviço. Na análise deve-se buscar por singularidades como:
    - Gargalos na infraestrutura;
    - Distribuição inapropriada dos recursos disponíveis;
    - Implementação ineficiente de aplicações;
    - Crescimento inesperado de taxas de transações;
    - Alocação e utilização ineficiente de memória;

A utilização de cada componente deve ser avaliada a curto, médio e longo prazo, e estabelecida os padrões de utilização máximo e mínimo nesses períodos.

- Otimização: A análise dos dados monitorados pode identificar áreas cuja utilização pode ser otimizada, melhorando o desempenho do serviço como um todo, técnicas de otimização incluem:
    - Balanceamento de Carga e Trafego;
    - Balanceamento de Trafego em Disco;
    - Uso Eficiente da Memória.

  Após a implementação de alguma dessas técnicas é necessário se proceder com o teste e validação;
- Modelagem: Uma atividade primária de Gestão de Capacidade é prever o comportamento de serviço de TI dado uma carga de serviço, tal fato pode ser conseguido por meio de modelagem do sistema. Simulações de eventos discretos podem antever problemas e auxiliar na alocação de recursos do serviço.

4.3.3.1 Recomendações para o risco de problemas de desempenho

Quanto mais flexível for a lógica de um serviço maior a capacidade de processamento que o mesmo demandará, uma vez que o mesmo deve se adaptar a diferentes cenários. Com uma interpretação maior de dados por parte da lógica do serviço os requisitos de desempenho para o mesmo são aumentados.

A fim de se garantir que o desempenho da infraestrutura de TI estará de acordo com as necessidades de execução do serviço, o fornecedor de serviços SOA deve ter uma visão ampla da infraestrutura de TI, por meio do monitoramento, análise, modelagem e otimização sistema. Todos os componentes críticos da infraestrutura devem ser considerados analisando-se dados relevantes para a capacidade de cada um. Deve ser buscado o monitoramento automático dos componentes, com sistemas de alarme acionando em pontos limite. Análises contínuas do comportamento e de tendências do sistema devem ser feitas, levantando-se distribuição inapropriada de recursos, aplicações ineficientes, crescimento inesperado de taxas de transações e uso ineficiente de memória, a fim de se verificar componentes da infraestrutura que prejudicam o desempenho do sistema como um todo.

4.3.3.2 Crítica à recomendação

Os principais desafios observados para lidar com a gestão de capacidade estão em providenciar previsões consistentes acerca do negócio, conhecimento de tecnologias atuais e futuras e habilidade em planejar e implementar a capacidade apropriada de TI para as necessidades do negócio. A providência de informações apropriadas para o planejamento e estratégia do negócio exige investimento em recursos, em conhecimento e treinamento de pessoal. Tal investimento nos recursos da organização pode não estar no alcance dos recursos da mesma. Vemos que o investimento em capacidade necessita de investimento financeiro e em conhecimentos, além de um planejamento prévio, tais características não podem ser adquiridas em um curto espaço de tempo.

4.3.4 - Risco 4 : Requisitos de acoplamento de múltiplos consumidores

Como visto na seção 3.2.3, consumidores de serviços têm necessidades diferentes, logo pode acontecer de determinado nível de abstração ser adequado a um consumidor, porém ser insuficiente para atender a requisitos de outro. A abstração de serviço influencia de forma direta a aplicabilidade e reuso de um serviço. Uma avaliação descabida do nível de abstração pode limitar a capacidade do consumidor de usar um serviço, prejudicando o reuso e trazendo insucesso ao mesmo.

Por meio da análise do escopo dos processos ITIL este risco foi mapeado no processo de Gerenciamento de Nível de Serviço, do ciclo de vida Desenho de Serviço. Este processo nos permite avaliar de forma precisa o nível de abstração e requisitos que a maioria dos consumidores precisam, podendo dessa forma otimizar a utilização dos recursos.

Gestão de Nível de Serviço é um nome dado ao processo de planejar, fazer acordos, projetar, coordenar, monitorar e produzir dados de Nível de Acordo de Serviço (SLA’s), para garantir que a qualidade do serviço seja mantida e gradualmente melhorada (ITIL, SERVICE DESIGN, 2007).

Tal processo não está envolvido somente com a gestão dos serviços atuais, mas também se preocupa em garantir que os requisitos futuros estimados também sejam considerados. Novos acordos de nível de serviço que sejam estabelecidos com base em um Gerenciamento de Nível de Serviço buscam garantir as necessidades e expectativas de negócio.

O propósito geral do Gerenciamento de Nível de Serviço é garantir que operações e desempenho de serviço sejam medidos de maneira consistente em toda a organização de TI, e

que os dados produzidos a partir da observação do sistema mostrem as necessidades dos negócios e dos consumidores.

Principais atividades propostas por ITIL

- Determinar, negociar, documentar e acordar requisitos para novos serviços, gerenciar e rever ao longo de toda a vida operacional do serviço se o mesmo está de acordo;
- Monitorar e medir o desempenho do serviço para todas as operações que envolvam os requisitos estabelecidos no acordo de nível de serviço;
- Coletar, medir e melhorar dados referentes à satisfação do consumidor;
- Promover revisão de serviços e instigar evoluções;
- Guardar e gerenciar todas as reclamações por parte dos clientes;

4.3.4.1 Recomendações para o risco de acoplamento de múltiplos usuários

Os diferentes requisitos de acoplamento dos múltiplos usuários de serviços SOA, trazem necessidades de níveis de abstração diferentes. O processo de Gerenciamento de Nível de Serviço ITIL faz com que o fornecedor de serviços SOA leve em consideração o nível de serviço que os consumidores tenham como necessidade. Buscando conhecer tal necessidade o fornecedor deve buscar informações com os consumidores, gerenciar reclamações dos mesmos, monitorar o desempenho dos serviços que envolvam os requisitos dos consumidores e por fim promover a evolução dos mesmos.

4.3.5 Risco 5 : Intepretação errada pelas pessoas devido ao excesso de abstração de serviço

Foi visto na seção 2.2.1.1, sobre o contrato de serviço, que este é o responsável por transmitir aos usuários os propósitos, capacidades e requisitos de serviços SOA. Para proporcionar um ambiente mais limpo ou mesmo não fornecer soluções proprietárias o princípio da abstração em SOA, faz com que determinadas informações sejam ocultadas do consumidor. O nível de abstração é uma opção do desenvolvedor do serviço. O risco surge quando tal nível é exagerado a ponto de não fornecer as informações suficientes para usuário optar pela utilização do serviço, prejudicando o reuso.

O risco foi mapeado no processo de Gerenciamento de Catálogo de Serviço, do ciclo de vida Desenho de Serviço de ITIL. Como visto anteriormente a proposta do processo de Gerenciamento de Catálogo de Serviço é providenciar uma única fonte consistente de

informação sobre todos os serviços, e garantir que a mesma seja amplamente disponível para aqueles que tenham permissão de acesso. O Catálogo de Serviço deve conter todos os detalhes de todos os serviços atualmente em uso. (ITIL, SERVICE DESIGN, 2007).

O objetivo do Gerenciamento de Serviço é garantir que o Catálogo de Serviço seja produzido e mantido, contendo informações consistentes e essenciais de todos os serviços.

Por meio dos métodos e atividades propostas pelo processo de Gerenciamento de Catálogo de Serviço, o gestor pode julgar o nível de abstração das informações que seja aceitável para o bom entendimento dos propósitos do serviço por parte dos potenciais usuários.

Processos Propostos por ITIL

- Definição do Serviço;
- Produção e manutenção de um Catálogo de Serviço consistente;
- Interfaces, dependências e consistência entre Catálogo de Serviço e Portfólio de Serviço;
- Interfaces e dependências entre todos os serviços, componentes suporte e itens de configuração;

Atividades Propostas por ITIL

- Acordos e documentação da definição do serviço entre todas as partes relevantes;
- Interfaceamento do Gerenciamento de Portfólio de Serviço com o Gerenciamento de Catálogo de Serviço;
- Produzir e manter o Catálogo de Serviço e seus recursos, em conjunto com o Portfólio de Serviço;
- Interfacemanto com grupos de suporte, fornecedores e Gerenciamento de Configuração, para acordo de Catálogo de Serviço Técnico;
- Interfaceamento com Gerenciamento de Relações de Negócios e Gerenciamento de Nível de Serviço para garantir que as informações estejam alinhadas com os negócios e processos de negócios.

4.3.5.1 Recomendações para o risco de intepretação errada por parte das pessoas

Sabemos que utilização do principio SOA de abstração de serviço é uma opção do desenvolvedor, o mesmo pode escolher o que deseja ocultar para o usuário. Tal abstração deve, contudo, buscar não ocultar informações que sejam essenciais para o consumidor de

serviço SOA fazer a correta interpretação de funcionalidades, capacidades e requisitos do serviço.

Para que o risco de interpretação errada por parte das pessoas não ocorra o fornecedor deve construir um catálogo de serviços que leve em consideração informações essenciais para o consumidor de serviços ter a correta interpretação dos mesmos. Para tal o fornecedor deve fazer acordos e documentação sobre definições do serviço entre todas as partes relevantes, promover reuniões com fornecedores e grupos de suporte para elaboração do catálogo de serviço técnico, promover reuniões com consumidores para buscar destes informações sobre a intepretação do contrato de serviços.

4.3.5.2 Crítica à recomendação

Verificamos que esta recomendação trata-se de, meramente selecionar a quantidade e qualidade de informações consistentes sobre o serviço, de forma que o consumidor possa fazer a correta interpretação. Tal recomendação é possível de ser implementada independentemente dos recursos financeiros que uma organização disponha. No entanto, demanda-se de tempo para se proceder como a correta avaliação do nível de informações a serem transmitidas no contrato.

4.3.6 Risco 6 : Preocupações com governança

Como visto na seção 3.2.4, quando uma porcentagem alta de um inventário de serviços é composta de ativos reutilizáveis, as abordagens de governança tradicionais não são mais aplicáveis. Os requisitos de governança que SOA traz exigem que a estrutura organizacional de ambientes de TI sejam expandidas, de forma a assegurar o uso e evolução apropriados do sistema (ERL, 2007). A ausência dessa estrutura pode fazer com que *designers* de serviços reutilizáveis tenham como preocupação apenas as necessidades das soluções cuja entrega imediata são responsáveis, não se preocupando quanto à evolução do sistema como um todo.

Depois de ser feita a análise dos processos de ITIL chegamos a conclusão de que este risco não está contido no escopo de apenas um ou dois processos do ciclo de vida ITIL. Uma boa governança para SOA seria conseguida com a aplicação de ITIL em seu contexto geral, aplicando-se cada um dos processos nas situações pertinentes. Não apenas considerações a respeito segurança de SOA devem ser consideradas, como é feito no escopo deste trabalho, mas todos os aspectos de SOA.

Tal consideração foi ilustrada nos artigos citados na introdução deste capitulo onde Xian-Peng , Bi-ying e Rui Fang (2012) e Susanti e Sembiring (2011) escreveram trabalhos

onde mostram como uma alternativa para governança SOA foi criada, mapeando-se cada um dos aspectos necessários para governança SOA com os processos do ciclo de vida ITIL.

4.3.6.1 Recomendações para o risco de preocupações com governança

Vimos que podemos fazer uma boa governança SOA a partir dos processos e atividades propostas por ITIL, porém para que tal governança seja feita é necessário que todo o escopo de ITIL e cada aspecto de SOA seja considerado. Seria recomendado para a organização fornecedora de serviços SOA o investimento em conhecimento por parte de seus gestores, da biblioteca ITIL, por meio de cursos e certificações, a utilização de consultores com conhecimento sobre as praticas ITIL também deve ser considerada.

4.3.6.2 Crítica à recomendação

A implantação de ITIL dentro de uma organização de TI pode ser uma característica bastante benéfica, uma vez que ITIL se trata de uma biblioteca de boas práticas na área de TI mais adotadas no mundo, sendo um excelente guia para o gestor conduzir a sua empresa. Porém, para se implantar ITIL na organização seria necessária a obtenção prévia de conhecimentos acerca da biblioteca, sendo necessário o investimento em conhecimento, além disso, uma equipe deveria ser formada na empresa com essa única finalidade. Dependendo do tamanho da empresa e o foco de mercado ao qual a mesma se dirige uma implantação de todo o escopo de ITIL pode se fazer dispendioso.

4.3.7 Risco 7: Preocupações com disponibilidade

Vimos na seção 3.2.4 que apesar de o reuso de serviços ser o foco principal de SOA, o mesmo pode trazer consigo, se não for bem gerenciando, o risco da indisponibilidade para todo o sistema, já que um único serviço pode representar um ponto de falha para vários processos ao mesmo tempo. Caso um serviço deixe de estar disponível por qualquer motivo (exemplo de indisponibilidade no host que o hospeda), todos os consumidores que dependem do mesmo terão suas operações interrompidas.

Analisado o escopo dos processos ITIL, mapeamos risco no processo de Gerenciamento de Disponibilidade, do ciclo de vida Desenho de Serviço, o qual tem o objetivo de garantir que o nível de disponibilidade esperada pelo consumidor seja mantida, ou mesmo excedida (ITIL, SERVICE DESIGN, 2007).

A forma de verificar se o nível de disponibilidade acordado está sendo obedecido é por meio do monitoramento e análise dos dados obtidos, onde o processo de Gerenciamento de Disponibilidade deve sempre estar buscando a otimização e proativamente melhorando a disponibilidade da infraestrutura de TI.

O escopo do processo de Gerenciamento de Disponibilidade cobre o projeto, implementação, gerenciamento e desenvolvimento dos componentes e serviços de TI, devendo levar em conta os requisitos de negócio dos processos correntes, requisitos futuros, desempenho de infraestrutura de TI, aplicações e plataformas. Tal processo de ITIL depende fortemente do monitoramento de serviços e componentes de TI no que diz respeito a aspectos de disponibilidade.

'*If you don't measure it, you can't manage it'*
'If you don't measure it, you can't improve it'
'If you don't measure it, you probably don't care'
'If you can't influence or control it, then don't measure it'

(ITIL, SERVICE DESIGN, 2007)

Duas categorias diferentes de atividades são propostas por ITIL, são elas:

- Projeto de disponibilidade: atividade relacionada ao projeto técnico do serviço de TI e alinhamento com fontes internas e externas para que sejam atingidos os requisitos de disponibilidade para o negócio. Deve incluir infraestrutura, ambiente, dados e aplicações;
- Mecanismos de recuperação: atividades relacionadas ao projeto de mecanismos que garantam que quando de uma falha em componentes ou serviço de TI, o sistema se reestabelecerá o mais rápido possível.

Processos Propostos por ITIL

- Determinar requisitos de disponibilidade que o mercado exige para os serviços de TI, de forma a formular critérios de disponibilidade e recuperação para os componentes de TI;
- Determinar as funções vitais para o negócio;
- Determinar os impactos consequentes de falha em serviços ou componentes de TI e onde apropriado, rever os critérios de projeto da disponibilidade, para providenciar dispositivos de resiliência adicional, de forma a minimizar os impactos nos negócios;
- Estabelecer medidas e formas de coletar dados a respeito disponibilidade que mostrem a perspectiva dos negócios e dos usuários;
- Monitorar e analisar a tendência de disponibilidade dos componentes de TI;

- Produzir e manter Plano de Disponibilidade que priorize e planeje melhoras para a disponibilidade dos serviços de TI;
- Atividades contínuas que busquem o aumento da disponibilidade dos serviços de TI;

Atividades Propostas por ITIL

- Busca por tecnologias tolerantes a falhas de forma a minimizar o impacto planejado ou não quando de uma falha em componentes;
- Duplexar ou providenciar componentes de infraestrutura de TI alternativos, para permitir que um componente reserva desempenhe a função de outro;
- Buscar uma maior confiança nos componentes de TI, por meio de regime de testes;
- Buscar melhores projetos e desevolvimento de *software*;
- Buscar melhores processos e procedimentos;
- Desenvolver a capacidade de pessoal com mais treinamento;

4.3.7.1 Recomendações para o risco de preocupação com disponibilidade

Questões relacionadas à disponibilidade têm sido cada vez mais consideradas nos dias de hoje, uma vez que soluções intolerante a falhas, como as que funcionam em transações bancárias, têm tido seu tráfego aumentado. SOA por sua vez faz com que a disponibilidade seja um princípio ainda mais discutido, uma vez que indisponibilidade de um único serviço pode fazer com que vários processos tenham sua operação prejudicada.

A fim de que o fornecedor de serviços SOA busque mitigar riscos de disponibilidade, o mesmo deve determinar requisitos de disponibilidade impostas pelo mercado para serviços de TI, e a partir desses estabelecer limites. De posse dos limites, deve ser feito o planejamento para a infraestrutura, buscando o uso se componentes robustos e tolerantes a falhas. A duplexação destes como meio de infraestrutura alternativa caso a principal falhe, a simulação de falhas para verificar o funcionamento dos dispositivos e aumentar a capacidade de pessoal por meio de treinamentos.

4.3.7.2 Crítica à recomendação

O aumento de disponibilidade nos serviços de TI tem sido uma das questões mais discutidas no ramo, uma vez que a disponibilidade é o aspecto que o consumidor mais busca. Sempre que financeiramente justificável uma organização deve investir em recursos para buscar garantir aumento de disponibilidade. O uso de componentes robusto, tolerantes a

falhas, assim como a duplexação desses pode ser financeiramente inviável para determinada organização, fato que pode tornar a recomendação com pouca aceitação.

4.3.8 Risco 8 : Preocupações com segurança

Foi visto na seção 3.2.4 que devido à capacidade de reuso de serviço em SOA, a preocupação com aspectos de desenvolvimento de software seguro tem se tornado cada vez maior, uma vez que um serviço criado sem levar em consideração tais aspectos pode proliferar suas vulnerabilidades por uma serie de processos que utilizam o mesmo. "*Reuso de um serviço vulnerável permite aos indivíduos mal intencionados a reutilizar estratégias de ataque*" (LOWIS e ACCOSI, 2011).

Gerenciamento de Segurança da Informação é hoje uma questão que precisa ser considerada em todo o *framework* de governança de uma corporação de TI. Segurança da Informação é uma atividade de gerenciamento que providencia as direções estratégicas para atividades seguras, e garante que os objetivos sejam atingidos. Garante também que os riscos sejam gerenciados e que recursos de informação da empresa sejam guardados. (ITIL, SEVICE DESIGN, 2007).

Para ITIL, os objetivos de segurança da informação são atingidos quando:

- A informação está disponível e é inteligível quando requisitada, o sistema que a providencia é apropriadamente resistente a ataques e se recupera de falhas (disponibilidade);
- A informação é observada somente por aquele que tem os direitos de conhecê-la (confidencialidade);
- A informação é completa, real e protegida contra modificações não autorizadas (integridade);
- Transações, assim como troca de informações entre empresas, podem ser confidenciais (autenticidade);

Como podemos ver o processo de Gerenciamento de Segurança da Informação de ITIL leva e conta os princípios para sistemas seguros vistos na seção 2.3.

Processos Propostos por ITIL

- A produção, manutenção, distribuição e imposição da Politica de Segurança da Informação;
- Entendimento dos requisitos de segurança atuais e futuros para o negócio assim como das Politicas de Segurança para o Negócio;

- Implementação de um conjunto de controles de segurança que suportem a Política de Segurança da Informação e gerencie riscos associados ao acesso a serviços, informação e sistemas;
- Gerenciamento de fornecedores e contratos a respeito acesso ao sistema e serviços;
- Monitoramento e gerenciamento de todas as brechas de segurança e incidentes associados a todos os sistemas e serviços;
- Analisar, produzir dados e buscar reduzir a quantidade e impactos ocasionados por brechas em segurança e incidentes;
- O desenvolvimento proativo de controles de segurança, e gerenciamento de riscos buscando a redução de riscos de segurança;
- Integração de aspectos de segurança com todos os outros processos de Gerenciamento de Segurança em TI;
- Agendamento de revisões de segurança, audições e testes de penetração.

Atividades Propostas por ITIL

Podemos observar as seguintes categorias de atividades ao longo do processo de Gerenciamento de Segurança da Informação em ITIL:

Preventivas

- Controle de direitos de acesso, concedendo, mantendo e retirando direitos;
- Autorizações de acesso, identificando a quem é permitido acesso, quais informações pode observar e ferramentas utilizar;
- Identificação e autenticação, confirmando quem está buscando acesso;
- Controle de Acesso, garantindo que só pessoas autorizadas conseguiram acesso;

Redutivas de danos quando um incidente ocorrer

- *Backups;*
- Desenvolvimento, teste e manutenção de plano de contingência.

Detecção de incidentes

- Monitoramento conciliado a dispositivos de alerta;
- Checagem de vírus com software antivírus.

4.3.8.1 Recomendações para o risco de preocupação com segurança

A implementação de aplicações seguras para SOA é um requisito de estrema relevância, uma vez que um serviço vulnerável irá proliferar suas vulnerabilidades ao longo

de soluções que utilize suas funcionalidades. Dessa forma para que um fornecedor de serviços SOA não coloque no mercado serviços vulneráveis e mesmo tenha sua reputação prejudicada, é necessário observância aos princípios de segurança da informação. Um documento com a política de segurança de informação da empresa deve ser produzindo, especificando os requisitos de segurança atendidos. Brechas de segurança devem ser buscas e monitoradas por meio de revisões, auditorias e testes de penetração, desenvolvimento proativo de controles de segurança e o acesso ao sistema deve ser totalmente controlado, por meio de controle de direitos e autorizações.

4.3.8.2 Críticas à recomendação

A fim de que serviços SOA seguros sejam produzidos, todo investimento em conhecimento, auditorias e testes na busca de brechas é justificável. Uma vez que os aspectos de disponibilidade, confidencialidade e integridade estão em risco quando não acontece a devida observância aos aspectos de segurança em aplicações.

4.3.9 Risco 9 : Preocupação com desenvolvimento ágil

Como visto na seção 3.2.4, a capacidade de reuso em SOA pode demandar de bastante recurso na implementação de serviços, principalmente recursos intelectuais, de tempo e dinheiro, a fim de que o pleno sucesso seja atingido. Análises detalhadas e considerações sobre diversos contextos em que o serviço deverá atuar devem ser observadas. Tal fato pode fazer com que empresas que tenham o desenvolvimento ágil como princípio não atinjam seus objetivos, pelo menos no período de transição para SOA, visto que após esta atingir sua maturidade, a produção de software se torna algo extremamente ágil, uma vez que os serviços já estarão implementados e apenas chamadas a estes serão necessárias.

Uma vez que se trata de um risco associado ao inicio ou transição para produção de serviços SOA e após análise do escopo dos processos ITIL, verificamos que este risco pode ser mapeado no processo de Planejamento e Suporte da Transição, do ciclo de vida Transição de Serviço de ITIL.

O processo de Planejamento e Suporte da Transição tem por propósito o planejamento apropriado de capacidade e recursos para se projetar, testar, implementar e estabelecer um novo ou fazer modificação de um serviço de TI. Este processo providencia suporte para a transição de grupos e pessoas, planeja as modificações necessárias para garantir a integridade de todos os ativos de serviço. Garantindo dessa forma que questões relacionadas à transição,

riscos e desvios sejam reportadas aos tomadores de decisão apropriados (ITIL, SERVICE TRANSITION, 2007).

Um efetivo Planejamento de Transição e Suporte pode melhorar significativamente as habilidades do provedor de serviços, para administrar grande quantidade de mudanças, melhorando o alinhamento dos planos entre consumidores, fornecedores e negócios (ITIL, SEVICE TRANSITION, 2007).

Podemos observar então que o objetivo do processo de Planejamento e Suporte da Transição é planejar e coordenar os recursos de forma a se atingir o sucesso em um novo ou na modificação de um serviço de TI, de forma a se cumprir custos, qualidade e tempos estimados. Com o processo pode-se garantir que todas as partes envolvidas adotem um *framework* de padrões de processos reusáveis comuns a fim de se desenvolver-se de forma eficaz e eficiente.

Processos Propostos por ITIL

- Incorporar projeto e requisitos de operação nos planos de transição;
- Gerenciamento e Operação de plano de transição e atividades suporte;
- Gerenciamento do progresso de Transição de Serviços, mudanças, riscos e desvios;
- Revisão de qualidade de todos os planos de implementação;
- Gerenciamento e operação de processos de transição, sistemas suporte e ferramentas;
- Comunicação com usuários, consumidores e *stakeholders;*
- Monitoramento e desenvolvimento da performance de transição de serviço.

Atividades Propostas por ITIL

- Descrever propostas e objetivos para a estratégia de transição;
- Verificar padrões aplicáveis, acordos, legislação, regulação e requisitos contratuais;
    - Padrões internos e externos;
    - Interpretação de legislação, guias industriais e outros requisitos impostos;
    - Acordos e contratos que se apliquem à transição de serviços;
- Reuniões e acordos entre organização (terceiros, parceiros estratégicos, fornecedores e provedores de serviço) e *stakeholders* envolvidos na transição;
- Elaborar um *framework* para a Transição de Serviço, contendo:
    - Políticas, processos e práticas aplicáveis para a transição de serviço incluindo interfaces com o provedor de serviços;
    - Papeis e responsabilidades;
    - Planejamento de recursos;
    - Preparação para transição e requisitos de treinamento;

    - Reuso de experiência organizacional, *expertise*, ferramentas, conhecimentos e dados históricos relevantes;
    - Compartilhamento de recursos e suporte;
- Elaboração de critérios para parada e recomeço de atividades de transição, cenários de falha e sucesso;
- Preparação de recursos humanos:
    - Fazer acordo de papeis e responsabilidades;
    - Acordar e agendar treinamentos e transferência de conhecimentos;
- Monitorar e avaliar o desenvolvimento da transição, cenários de falha e sucesso;

4.3.9.1 Recomendações para o risco de preocupação com desenvolvimento ágil

Em uma transição para SOA, uma empresa cujo princípio seja a produção ágil de software deve ter em mente que a produção de serviços com reuso demanda de tempo e recursos, a ponto de prejudicar a produção ágil. Buscando minimizar os impactos na agilidade de produção a empresa deve elaborar estratégia de transição, descrevendo propostas e objetivos, podendo assim gerenciar a transição, riscos e desvios.

Devem ser promovidas reuniões e acordos entre organização (terceiros, parceiros estratégicos, fornecedores e provedores de serviço) e *stakeholders* envolvidos na transição. O reuso de experiência organizacional, *expertise*, ferramentas, conhecimentos e dados históricos relevantes devem ser considerados, assim como o treinamento e transferências de conhecimentos por meio de cursos para os desenvolvedores de aplicações.

Por fim o reuso de experiências, treinamentos e utilização de padrões de desenvolvimento poderão agilizar a produção de serviços SOA. No entanto é preciso ter em mente que uma plataforma SOA madura não pode ser desenvolvida da noite para o dia. A transição para o paradigma SOA de ser planejada e monitorada, e um tempo deve ser estimado para que a mesma possa começar atingir os requisitos de agilidade necessários ao fornecedor de serviços.

4.3.9.2 Crítica à recomendação

Vemos que esta recomendação busca o reuso de experiências, *expertise*, ferramentas e o treinamento de pessoal para a produção ágil de software, portanto, trata-se de uma recomendação que não é aplicável em qualquer contexto. É necessário extremo cuidado para que a agilidade na produção das soluções não faça com que a qualidade do serviço seja

comprometida, com questões relacionadas à segurança, capacidade e disponibilidade sendo deixadas de lado. É possível se concluir que, para uma organização iniciando um projeto SOA, é necessário implantar a tecnologia e progredir na produção de serviços. O amadurecimento desta iria se encarregar por si só na entrega ágil de software.

4.3.10 Risco 10: Aplicar o princípio da visibilidade após a implementação do serviço

Um dos fatos que fez com a que a aceitação de SOA fosse tão ampla foi o reuso de serviço. Requisito fundamental para que o reuso aconteça é o conhecimento de funcionalidades, capacidades e requisitos dos serviços por parte dos clientes, como dita o princípio da visibilidade. Como visto na seção 3.2.5 o risco de se aplicar tal princípio somente após a implementação do serviço está no fato da perda de detalhes da funcionalidade do serviço por esquecimento, uma vez que detalhes podem passar despercebidos na fase de documentação. Os próprios desenvolvedores do serviço têm os detalhes minuciosos do mesmo, logo estes seriam os mais indicados para fazer o esboço do princípio de visibilidade concomitantemente com a implementação do serviço.

Tendo em vista a mitigar o risco de que um serviço não ser reutilizado devido à falta de informação em seus documentos, mapeamos o mesmo no processo de Gerenciamento de Catálogo de Serviço, do ciclo de vida Desenho de Serviço de ITIL.

A proposta do processo de Gerenciamento de Catálogo de Serviço é providenciar uma única fonte consistente de informação sobre todos os serviços, e garantir que a mesma seja amplamente disponível para aqueles que tenham permissão de acesso. O Catálogo de Serviço deve conter todos os detalhes de todos os serviços atualmente em uso. (ITIL, SERVICE DESIGN, 2007).

Processos Propostos por ITIL

- Definição do Serviço;
- Produção e manutenção de um Catálogo de Serviço consistente;
- Interfaces, dependências e consistência entre Catálogo de Serviço e Portfólio de Serviço;
- Interfaces e dependências entre todos os serviços, componentes suporte e itens de configuração;

Atividades Propostas por ITIL

- Acordos e documentação da definição do serviço entre todas as partes relevantes;

- Interfaceamento do Gerenciamento de Portfólio de Serviço com o Gerenciamento de Catálogo de Serviço;
- Produzir e manter o Catálogo de Serviço e seus recursos, em conjunto com o Portfólio de Serviço;
- Interfacemanto com grupos de suporte, fornecedores e Gerenciamento de Configuração, para acordo de Catálogo de Serviço Técnico;
- Interfaceamento com Gerenciamento de Relações de Negócios e Gerenciamento de Nível de Serviço para garantir que as informações estejam alinhadas com os negócios e processos de negócios.

4.3.10.1 Recomendações para o risco de aplicação do princípio da visibilidade após a implementação do serviço

A visibilidade de um serviço SOA é fundamental para que o mesmo seja percebido, que os usuários conheçam suas funcionalidades e as juguem necessárias para suas soluções. Um dos riscos associados a SOA está no fato de o princípio da visibilidade ser aplicado somente após a implementação do serviço, alguns detalhes de requisitos e funcionalidades podem passar despercebidos, pelo responsável pela documentação. O ideal é que o próprio desenvolvedor da aplicação no momento em que estiver escrevendo o código do programa, já busque documentar cada uma das partes. Porém na hipótese de o serviço SOA ter que ser documentado após a implementação podemos utilizar as práticas propostas pelo processo de Gerenciamento de Catálogo de Serviço de ITIL.

Durante a produção do Catálogo de Serviço acordos e documentações devem ser feitos entre todas as partes interessadas para as definições do serviço, deve haver o interfaceamento entre fornecedores e grupos suporte a fim de produção do catálogo de serviço técnico, encontros com os consumidores devem ser providenciados, a fim de que sejam buscadas destes informações a respeito a percepção dos mesmos acerca das funcionalidades do serviço. Dessa forma podem-se planejar melhor as informações contidas no catálogo de serviço e se essas são suficientes para a intepretação por parte dos potenciais usuários.

4.3.10.2 Crítica à recomendação

Buscamos nesta recomendação uma forma de se tentar produzir o catálogo de serviço o mais conciso possível, para que todas as funcionalidades do serviço constem no mesmo. Porém o ideal é que durante a fase de implementação do código, os próprios desenvolvedores busquem fazer a correta documentação do mesmo. É importante o investimento em

conhecimento de ferramentas que produzem automaticamente a documentação, a partir de comentários deixados no próprio código. A cultura de se expressar as informações necessárias para a documentação nos comentários do código deve ser difundida na organização. Com essa abordagem a empresa ganharia em agilidade e eficiência na documentação.

4.3.11 Risco 11: Utilizar linguagem de difícil intepretação no contrato de serviço

Como visto na revisão de literatura, o princípio da visibilidade SOA é primordial para que o contrato de serviço seja interpretado pelos usuários e o reuso de serviços, principal objetivo de SOA, aconteça de forma plena. Portanto trata-se de um risco a utilização de uma linguagem de difícil interpretação no contrato de serviços, uma vez que os consumidores na maioria das vezes não tem o mesmo grau de perícia técnica daqueles que implementaram o serviço SOA. A dificuldade de interpretação do contrato de serviço por parte de usuários poderia comprometer o reuso de um serviço com bons propósitos e funcionalidades.

Este risco de SOA pode ser mitigado por meio do mapeamento no processo de Gerenciamento de Catálogo de Serviço, do ciclo de vida Desenho de Serviço de ITIL. Como visto anteriormente, a proposta do processo de Gerenciamento de Catálogo de Serviço é providenciar uma única fonte consistente de informação sobre todos os serviços, e garantir que a mesma seja amplamente disponível para aqueles que tenham permissão de acesso. O Catálogo de Serviço deve conter todos os detalhes de todos os serviços atualmente em uso. (ITIL, SERVICE DESIGN, 2007).

O Catálogo de Serviços providencia uma fonte central de informação para os serviços de TI entregue pelas organizações provedoras. Ele garante que todas as áreas do negócio possam ver uma correta e consistente ilustração dos serviços de TI, juntamente com seus detalhes. Deve conter de forma clara uma interface entre usuários e serviço, como os serviços são utilizados, assim como o nível de qualidade que o consumidor pode esperar.

Tendo em vista o uso da linguagem de fácil interpretação por parte dos potenciais usuários de serviço o fornecedor deve se atentar com foco para as seguintes atividades, dentre as propostas por ITIL no processo de Gerenciamento de Catálogo de Serviço:

- Interfacemanto com grupos de suporte, fornecedores e Gerenciamento de Configuração, para acordo de Catalogo de Serviço Técnico;
- Interfaceamento com Gerenciamento de Relações de Negócios e Gerenciamento de Nível de Serviço para garantir que as informações estejam alinhadas com os negócios e processos de negócios.

4.3.11.1 Recomendações para o risco de utilização de linguagem de difícil interpretação no contrato de serviços

Visto que a interpretação do contrato de serviço é primordial pra que um bom serviço SOA tenha chance de reuso, o fornecedor deve buscar a utilização de uma linguagem de fácil entendimento por parte dos potenciais usuários dos serviços. Deve-se considerar o fato de que esses podem não ter o mesmo grau de conhecimento a cerca do desenvolvimento de software daqueles que estão implementando o serviço. A recomendação baseada nos processos de ITIL para utilização de fácil interpretação por parte de pessoas segue a mesma recomendação dada para o princípio da visibilidade no qual um Catálogo de Serviços conciso sobre todos os serviços SOA disponíveis deve ser elaborado.

A fim de se buscar a utilização de linguagem adequada, o gestor deve participar de encontros com fornecedores, grupos de suporte e com usuários a fim de que seja acordada a linguagem, e se a intepretação das informações estão sendo atendidas. Em caso negativo, adequação deve ser feita.

4.3.11.2 Crítica à recomendação

Esta recomendação consiste em meramente se transmitir para o consumidor uma linguagem adequada, a fim de que o mesmo possa interpretar a correta funcionalidade e requisitos do serviço. Vemos que tal recomendação além de essencial para a vida da empresa pode ser aplicada qualquer que seja o porte da organização, uma vez que esta deve apenas buscar com o consumidor ou acordar com parceiros o nível de linguagem adequado e utilizar o mesmo em seus documentos.

4.3.12 Risco 12: Serviço membro de composição como único ponto de falha em cascata

Vimos na seção 2.2.1.7, sobre a composição de serviços SOA, que o reuso de serviço nos possibilita compor um serviço maior contendo vários serviços com funcionalidades menores. Cada serviço faz o seu processamento e passa o resultado de sua saída para o outro. O risco nessa arquitetura é que um único serviço que tiver sua disponibilidade prejudicada pode afetar toda a composição. Um serviço pode ser membro de várias composições ao mesmo tempo, logo todas essas poderiam ser afetadas no caso de falha neste serviço.

Para mitigarmos esse risco devemos buscar recomendações para aumentar disponibilidade e continuidade do serviço. Dentre os processos ITIL temos os processos de Gerenciamento de Disponibilidade e Gerenciamento de Continuidade de Serviços de TI, do

ciclo de vida Desenho de Serviço. Ambos aplicados em conjunto proporcionarão o objetivo desejado.

O objetivo de Gerenciamento de Disponibilidade é garantir que o nível de disponibilidade de serviço entregue, esteja de acordo ou exceda o nível estabelecido. A proposta é providenciar um ponto de foco e gerenciamento para todas as questões de disponibilidade, relacionadas a serviços e recursos, garantindo que os propósitos de disponibilidade sejam medidos e atingidos (ITIL, SERVICE DESIGN, 2007).

O objetivo do Gerenciamento de Continuidade de Serviços de TI por sua vez é dar suporte a todo o contexto de Gerenciamento de Continuidade dos Negócios, garantindo que as instalações técnicas e de serviços de TI (incluindo sistemas operacionais, redes, aplicações, dados, repositórios, telecomunicações, suporte técnico) possam ser utilizadas e recomeçadas quando requisitado (ITIL, SERVICE DESIGN, 2007).

Tecnologia é um componente essencial para muitos processos de negócio hoje, continuidade e disponibilidade de TI se tornaram questões críticas para a sobrevivência dos negócios como um todo. Para garantir que os níveis acordados de continuidade e disponibilidade sejam atingidos deve-se proceder com medidas de redução de riscos e opções de recuperação rápida quando falhas ocorrem. De forma a buscar o correto gerenciamento buscamos as recomendações pertinentes à disponibilidade e continuidade em ITIL.

Processos Propostos por ITIL

Disponibilidade

- Determinar requisitos de disponibilidade que o mercado exige para os serviços de TI, de forma a formular critérios de disponibilidade e recuperação para os componentes de TI;
- Determinar as funções vitais para o negócio;
- Determinar os impactos consequentes de falha em serviços ou componentes de TI e, onde apropriado, rever os critérios de projeto da disponibilidade, para providenciar dispositivos de resiliência adicional de forma a minimizar os impactos nos negócios;
- Estabelecer medidas e formas de coletar dados a respeito disponibilidade que mostrem a perspectiva dos negócios e dos usuários;
- Monitorar e analisar a tendência de disponibilidade dos componentes de TI;
- Produzir e manter Plano de Disponibilidade que priorize e planeje melhoras para a disponibilidade dos serviços de TI;
- Atividades contínuas que busquem o aumento da disponibilidade dos serviços de TI;

Continuidade

- Acordos de escopo de gerenciamento de continuidade de serviços de TI e políticas adotadas;
- Análise de impacto para o negócio para quantificar o impacto de perdas que TI traria ao negócio;
- Análise de risco, para identificar potenciais riscos e ameaças para a continuidade, e probabilidade de ameaças se tornarem reais.
- Produção de plano de gerenciamento de continuidade de serviço de TI;
- Teste dos planos de gerenciamento;
- Manutenção dos planos de gerenciamento.

Atividades Propostas por ITIL

Disponibilidade

- Busca por tecnologias tolerantes a falhas de forma a mascarar o impacto planejado ou não quando de uma falha em componentes;
- Duplexar ou providenciar componentes de infraestrutura de TI alternativos, para permitir que um componentes reserva desempenhe a função de outro;
- Buscar uma maior confiança nos componentes de TI, por meio de regime de testes;
- Buscar melhores projetos e desevolvimento de *software*;
- Buscar melhores processos e procedimentos;
- Desenvolver a capacidade de pessoal com mais treinamento;

Continuidade

- Instalação de *nobreak* e *backup* de potência para computadores;
- Sistemas tolerantes a falhas para aplicações críticas, onde mesmo mínimas quedas no sistema não são aceitas;
- Uso de *RAID* e espelhamento de disco (*disk mirroring)* para servidores de LAN, de forma a prevenir perda, e garantir disponibilidade de dados;
- Equipamentos e componentes livres de reserva, para serem usados em caso de falha de outros equipamentos;
- Eliminação de Pontos Únicos de Falha, como redes de único ponto de acesso ou única fonte de potência para o prédio;
- Uso de sistemas e redes com implementação de mecanismos de resiliência;
- Maior controle de segurança físico e para componentes de TI;

- Controles eficazes para detectar interrupção de serviços, ou riscos a esses, mesmo para riscos ao ambiente físico;
- Uma estratégia de *backup* e recuperação compreensiva, incluindo armazenamento em locais físicos diferentes.

4.3.12.1 Recomendações para o risco de único ponto de falha em composição

A TI tem se tornado recurso crítico para diversas aplicações, em algumas delas não tolerando a mínima falha, os recursos devem ser contínuos e estar disponíveis sempre que requisitados. Para garantir que os níveis acordados de continuidade e disponibilidade sejam atingidos deve-se proceder com medidas de redução de riscos e opções de recuperação rápida quando falhas ocorrem. Um único serviço SOA que tiver disponibilidade prejudicada, irá causar impacto em diversas composições de que fizer parte. Buscando minimizar os riscos de falta de disponibilidade e continuidade para composições SOA, trazemos as recomendações baseadas nos processos de Gerenciamento de Disponibilidade e Gerenciamento de Continuidade dos Serviços de TI de ITIL. As recomendações devem ser consideradas em cada um dos serviços membros da composição, para que pontos únicos de falhas sejam minimizados.

Primeiramente o gestor deve determinar requisitos de disponibilidade impostos pelo mercado, para de posse desses possa fazer seu planejamento. Funções vitais para o funcionamento da infraestrutura devem ser listadas e documentadas. A utilização de componentes robustos à prova de falhas deve sempre ser buscada, assim como a duplexação de componentes reservas. A utilização de dispositivos de monitoramento para os componentes da infraestrutura e análise das tendências, uso de backup de dados em locais físicos diferentes. Mecanismos de resiliência devem ser projetados, para que a rede seja tolerante a falhas. Por fim pesquisas com usuários devem ser regularmente feitas para que a satisfação dos mesmos diante dos serviços seja analisada.

4.3.12.2 Crítica à recomendação

O aumento de disponibilidade nos serviços de TI tem sido uma das questões mais discutidas no ramo, uma vez que a disponibilidade é o aspecto que o consumidor mais busca. A tecnologia SOA, quando utiliza de composições leva esta questão a tona, uma vez que falta de disponibilidade ou continuidade em um único serviço prejudica todas as composições das quais ele faz parte. Sempre que financeiramente justificável uma organização deve investir em recursos para buscar garantir aumento de disponibilidade. O uso de componentes robusto,

tolerantes a falhas, assim como a duplexação desses pode ser financeiramente inviável para determinada organização, fato que pode tornar a recomendação com pouca aceitação, ou mesmo de uso financeiramente inviável.

4.3.13 Risco 13: Membros de composição como gargalo de desempenho

Como visto na seção 3.2.6, a composição de serviços SOA pode sofrer problema de desempenho ocasionado pela ineficiência de um único serviço membro, uma vez que os demais membros necessitam do processamento deste para dar continuidade às suas funcionalidades. Para que tal ineficiência não prejudique todo o sistema é necessário que seja avaliado o tempo de resposta de cada serviço, para os tráfegos requisitados.

Devemos dimensionar os recursos de forma a termos uma melhor relação custo benefício. Com base no escopo dos processos ITIL foi feito o mapeamento deste risco em dois processos diferentes, são eles: Gerenciamento de Capacidade, dentro do ciclo de vida Desenho de Serviço, e Gerenciamento de Demanda, dentro do ciclo de vida Estratégia de Serviço ITIL.

O grande desafio em lidar com a Gestão de Capacidade está em entender o relacionamento entre demanda e os requisitos do negócio, traduzindo essas em termos de avaliação de impactos e efeitos na utilização dos serviços (ITIL, SEVICE DESIGN, 2007).

A Gestão de Capacidade deve ser o ponto focal quando se busca a performance e capacidade dos recursos de TI, no que diz respeito a recursos de *hardware* e *software* .

Alinhada com a Gestão de Capacidade deve estar a Gestão de Demanda uma vez que esta deverá dimensionar qual o nível de capacidade coerente para o sistema, o mesmo não deve ter falta de capacidade para prover serviços, como também não deve ter excesso, para que recursos não sejam desperdiçados.

O Interfaceamento entre os processos de Gestão de Capacidade e Gestão de Demanda ITIL permite garantir que recursos de TI sejam planejados e implementados de forma a providenciar um nível consistente de serviço que seja atrelado às necessidades de desempenho atuais e futuras.

Processos e Técnicas Propostas por ITIL

- Antever questões de desempenho, tomando as ações necessárias antes que problemas ocorram;

- Verificar tendências na utilização dos componentes atualmente em funcionamento e estimar os requisitos futuros, usando limiares para planejar evoluções e melhoramentos;
- Modelar previamente as mudanças nos serviços de TI, avaliando pontos críticos na infraestrutura e aplicação para garantir o desempenho do serviço;
- Sempre que financeiramente justificável buscar o aumento do desempenho do serviço;
- Otimizar o desempenho de serviços e componentes;
- Monitorar, medir, produzir dados e rever o desempenho corrente de serviços e componentes;

Atividades Propostas por ITIL

- Monitoramento do Serviço: É importante que os dispositivos de monitoramento coletem todos os dados necessários para o processo de Gestão de Capacidade, dados típicos monitorados são:
    - Utilização do Processador;
    - Utilização de Memória;
    - Utilização de Dispositivos;
    - Tamanho de Filas;
    - Utilização de Disco;
    - Tempo de Resposta;
    - Uso de Dados;
    - Taxa de Conflitos;
    - Numero de Usuários no Sistema;
    - Taxa de Tráfego na Rede.

  Sistemas de alarme são importantes para quanto algum dos dados coletados estiverem próximo do valor limite estabelecido.
- Análise: Os dados coletados no monitoramento devem ser analisados de forma a se verificar tendências na utilização do serviço. Na análise deve-se buscar por singularidades como:
    - Gargalos na infraestrutura;
    - Distribuição inapropriada dos recursos disponíveis;
    - Implementação ineficiente de aplicações;
    - Crescimento inesperado de taxas de transações;
    - Alocação e utilização ineficiente de memória;

  A utilização de cada componente deve ser avaliada a curto, médio e longo prazo, e estabelecida os padrões de utilização máxima e mínima nesses períodos.

- Otimização: A análise dos dados monitorados pode identificar áreas cuja utilização pode ser otimizada, melhorando o desempenho do serviço como um todo, técnicas de otimização incluem:
    - Balanceamento de Carga e Trafego;
    - Balanceamento de Trafego em Disco;
    - Uso Eficiente da Memória.

  Após a implementação de alguma dessas técnicas é necessário se proceder com o teste e validação;
- Modelagem: Uma atividade primária de Gestão de Capacidade é prever o comportamento de serviço de TI dado uma carga de serviço, tal fato pode ser conseguido por meio de modelagem do sistema. Simulações de eventos discretos podem antever problemas e auxiliar na alocação de recursos do serviço.

4.3.13.1 Recomendações para o risco de membro de composição como gargalo de desempenho

Devido à possibilidade de reuso SOA, podemos combinar funcionalidades de diferentes serviços por meio de composições. Dentre os riscos do uso de diferentes serviços em composições temos o do desempenho, onde um único serviço membro pode prejudicar a eficiência de todo o sistema. O tempo de resposta de cada serviço SOA deve ser avaliado, considerando-se a demanda para o serviço é preciso dimensionar a capacidade de trafego do mesmo.

A recomendação para este risco foi baseada nos processos de Gerenciamento de Demanda e Gerenciamento de Capacidade de ITIL. Dispositivos de monitoramento e medição devem ser instalados em todos os componentes críticos da infraestrutura, análise da tendência na operação de cada um deve ser considerada, buscando-se por gargalos de desempenho, modelagem do sistema para pontos críticos de operação devem ser analisadas. Sempre que possível deve ser feito investimento em melhoria de capacidade para a infraestrutura, otimização deve ser buscada por meio da análise dos resultados de monitoramento dos componentes, utilização de tecnologias e atualização do gestor para técnicas de uso eficientes dos componentes.

4.3.13.2 Crítica à recomendação

Os principais desafios observados para lidar com a gestão de capacidade estão em providenciar previsões consistentes acerca do negócio, conhecimento de tecnologias atuais e

futuras e habilidade em planejar e implementar a capacidade apropriada de TI para as necessidades do negócio. A providência de informações apropriadas para o planejamento e estratégia do negócio exige investimento em recursos, em conhecimento e treinamento de pessoal. Tal investimento nos recursos da organização pode não estar no alcance dos recursos da mesma. Vemos que o investimento em capacidade necessita de investimento financeiro e em conhecimentos, além de um planejamento prévio, tais características não podem ser adquiridas em um curto espaço de tempo.

4.3.14 Risco 14: Exigência de maior desempenho em tempo de serviço

Verificamos na seção 3.2.7 que uma das soluções para se implementar a independência de estado de serviços consiste na delegação para um outro membro da arquitetura, como um banco de dados, para fazer a guarda da informação de estado. Porém a utilização desse banco de dados pode fazer com que o tenhamos uma maior exigência de desempenho por parte do serviço, uma vez que este demandaria de parte do poder de processamento para atualizar, manter, processar e interpretar informações de estado no banco de dados.

Afim de não comprometer a infraestrutura de TI, gerando problemas de disponibilidade e continuidade, deve-se fazer o correto dimensionamento de componentes, levando em consideração, inclusive, a situação do risco de maior exigência de desempenho em tempo de serviço. Para mitigar possíveis problemas causados por esse risco, mapeamos o mesmo nos processos de Gerenciamento de Demanda, do ciclo de vida Estratégia de Serviço, e de Gerenciamento de Capacidade, do ciclo de vida Desenho de Serviço.

O grande desafio em lidar com a Gestão de Capacidade está em entender a o relacionamento entre demanda e requisitos do negócio, e traduzi-los em termos de avaliação de impactos e efeitos na utilização dos serviços (ITIL, SEVICE DESIGN, 2007).

Alinhada com a Gestão de Capacidade deve estar a Gestão de Demanda uma vez que esta deverá dimensionar qual o nível de capacidade coerente para o sistema. O mesmo não deve ter falta de capacidade para prover serviços, como também não deve ter excesso, para que recursos não sejam desperdiçados.

A Interface entre os processos de Gestão de Capacidade e Gestão de Demanda ITIL permite garantir que recursos de TI sejam planejados e implementados de forma a providenciar um nível consistente de serviço que seja atrelado às necessidades de desempenho atuais e futuras.

Processos e Técnicas Propostas por ITIL

- Verificar tendências na utilização dos componentes atualmente em funcionamento e estimar os requisitos futuros, usando limiares para planejar evoluções e melhoramentos;
- Modelar previamente as mudanças nos serviços de TI, avaliando pontos críticos na infraestrutura e aplicação para garantir o desempenho do serviço;
- Sempre que financeiramente justificável buscar o aumento do desempenho do serviço;
- Otimizar o desempenho de serviços e componentes;
- Monitorar, medir, produzir dados e rever o desempenho corrente de serviços e componentes;

Atividades Propostas por ITIL

- Monitoramento do Serviço: É importante que os dispositivos de monitoramento coletem todos os dados necessários para o processo de Gestão de Capacidade, dados típicos monitorados são:
    - Utilização do Processador;
    - Utilização de Memória;
    - Utilização de Dispositivos;
    - Tamanho de Filas;
    - Utilização de Disco;
    - Tempo de Resposta;
    - Uso de Dados;
    - Taxa de Conflitos;
    - Numero de Usuários no Sistema;
    - Taxa de Tráfego na Rede.

  Sistemas de alarme são importantes para quanto algum dos dados coletados estiverem próximo do valor limite estabelecido.
- Análise: Os dados coletados no monitoramento devem ser analisados de forma a se verificar tendências na utilização do serviço. Na análise deve-se buscar por singularidades como:
    - Gargalos na infraestrutura;
    - Distribuição inapropriada dos recursos disponíveis;
    - Implementação ineficiente de aplicações;
    - Crescimento inesperado de taxas de transações;
    - Alocação e utilização ineficiente de memória;

A utilização de cada componente deve ser avaliada a curto, médio e longo prazo, e estabelecida os padrões de utilização máxima e mínima nesses períodos.

- Otimização: A análise dos dados monitorados pode identificar áreas cuja utilização pode ser otimizada, melhorando o desempenho do serviço como um todo, técnicas de otimização incluem:
    - Balanceamento de Carga e Trafego;
    - Balanceamento de Tráfego em Disco;
    - Uso Eficiente da Memória.

  Após a implementação de alguma dessas técnicas é necessário se proceder com o teste e validação;
- Modelagem: Uma atividade primária de Gestão de Capacidade é prever o comportamento de serviço de TI dado uma carga de serviço, tal fato pode ser conseguido por meio de modelagem do sistema. Simulações de eventos discretos podem antever problemas e auxiliar na alocação de recursos do serviço.

4.3.14.1 Recomendações para o risco de exigência de maior desempenho

A fim de se aumentar a independência de Estado de Serviço de serviços SOA, recursos como a delegação para uma outra parte da arquitetura para a guarda da informação de estados são utilizados. Visto que um número muito grande seções do serviço podem estar atendendo a diferentes chamados ao mesmo tempo, a utilização desse recurso pelo serviço pode exigir maiores requisitos de desempenho para o mesmo, uma vez que parte do processamento será utilizado somente para busca, guarda e interpretação de informações de estado no banco de dados. A fim de monitorar a necessidade de aumento nos recursos para que problemas de desempenho não afetem a operação do serviço, formulamos recomendações baseadas nos processos de Gerenciamento de Capacidade e Gerenciamento de Demanda de ITIL.

O monitoramento, assim como a análise de comportamento para os componentes da infraestrutura de TI devem ser de extrema importância para se verificar a exigência de maior capacidade dos recursos, modelagens e simulações devem também ser consideradas, a fim de se antever problemas de desempenho na rede. Devem-se estabelecer valores limite de acordo com as observações para o tempo de resposta do banco de dados, tamanho de filas, utilização do disco, taxa de tráfego na rede.

4.3.14.2 Crítica à recomendação

Os principais desafios observados para lidar com a gestão de capacidade estão em providenciar previsões consistentes acerca do negócio, conhecimento de tecnologias atuais e futuras e habilidade em planejar e implementar a capacidade apropriada de TI para as necessidades do negócio. A providência de informações apropriadas para o planejamento e estratégia do negócio exige investimento em recursos, em conhecimento e treinamento de pessoal. Tal investimento nos recursos da organização pode não estar no alcance dos recursos da mesma. Vemos que o investimento em capacidade necessita de investimento financeiro e em conhecimentos, além de um planejamento prévio, tais características não podem ser adquiridas em um curto espaço de tempo.

4.4- Recomendações gestão de risco de SOA baseadas na biblioteca ITIL

Esta seção irá reunir todas as recomendações baseadas nos processos de ITIL propostas na seção 4.3 para mitigar os riscos apresentados para SOA.

4.4.1 Recomendação 1: Controle de versão de serviços SOA

A fim de se gerenciar o controle de versão de serviços SOA deve-se produzir um catálogo de serviços consistente e documentado. Para se produzir tal catálogo trazendo o nível de detalhamento que proporcione a correta interpretação das funcionalidades, e requisitos das diferentes versões do serviço, deve-se buscar o auxilio de grupos de suporte, fornecedores, assim como periodicamente se proceder com pesquisas a usuários dos serviços, buscando compreender como os mesmos conseguem enxergar o serviço, apenas por meio da interpretação da documentação do mesmo. Garantimos dessa forma que o nível de informações transmitidas aos potenciais consumidores do serviço sejam suficientes para que os mesmos possam fazer a escolha certa quando estiver procurando por um serviço.

4.4.2 Recomendação 2: Conhecimento de novas tecnologias

A fim de que um fornecedor de serviços SOA não corra o risco de ter a operação de algum serviço inviabilizada por dependência de tecnologia, o mesmo deve verificar tendências e realizar testes na operação dos atuais componentes do sistema. Requisitos futuros devem também ser estimados, para assim se fazer o correto planejamento de sistemas novos. Para se proceder com tal verificação e análise do cenário, o fornecedor se serviços SOA deve sempre buscar a atualização de seus conhecimentos a respeito da tecnologia, buscando informações em literatura profissional e participando de reuniões, congressos, conferências,

onde concentrará potenciais fornecedores e parceiros de negócio, e o tema em questão será discutido.

4.4.3 Recomendação 3: Dimensionamento de desempenho

Quanto mais flexível for a lógica de um serviço maior a capacidade de processamento que o mesmo demandará, uma vez que o mesmo deve se adaptar a diferentes cenários. Com uma interpretação maior de dados por parte da lógica do serviço os requisitos de desempenho para o mesmo são aumentados.

A fim de se garantir que o desempenho da infraestrutura de TI estará de acordo com as necessidades de execução do serviço, o fornecedor de serviços SOA deve ter uma visão ampla da infraestrutura de TI, por meio do monitoramento, análise, modelagem e otimização sistema. Todos os componentes críticos da infraestrutura devem ser considerados analisando-se dados relevantes para a capacidade de cada um. Deve ser buscado o monitoramento automático dos componentes, com sistemas de alarme acionando em pontos limite. Análise contínua do comportamento e verificação de tendências deve ser feitas, levantando-se distribuição inapropriada de recursos, aplicações ineficientes, crescimento inesperado de taxas de transações e uso ineficiente de memória, a fim de se verificar componentes da infraestrutura que prejudicam o desempenho do sistema como um todo.

4.4.4 Recomendação 4: Conhecer as necessidades dos múltiplos clientes

Os diferentes requisitos de acoplamento dos múltiplos usuários de serviços SOA, trazem necessidades de níveis de abstração diferentes. O processo de Gerenciamento de Nível de Serviço ITIL faz com que o fornecedor de serviços SOA leve em consideração o nível de serviço que os consumidores tenham como necessidade. Tendo em vista conhecer tal necessidade o fornecedor deve buscar informações com os consumidores, gerenciar reclamações dos mesmos, monitorar o desempenho dos serviços que envolvam os requisitos dos consumidores e por fim promover a evolução dos mesmos.

4.4.5 Recomendação 5: Catálogo de serviço que proporcione correta interpretação das funcionalidades e requisitos dos serviços SOA

Sabemos que utilização do princípio SOA de abstração de serviço é uma opção do desenvolvedor, o mesmo pode escolher o que deseja ocultar para o usuário. Tal abstração deve, contudo, buscar não ocultar informações que sejam essenciais para o consumidor de

serviço SOA fazer a correta interpretação de funcionalidades, capacidades e requisitos do serviço.

Para que o risco de interpretação errada por parte das pessoas não ocorra o fornecedor deve construir um catálogo de serviços que leve em consideração informações essenciais para o consumidor de serviços ter a correta interpretação dos mesmos. Para tal o fornecedor deve fazer acordos e documentação sobre definições do serviço entre todas as partes relevantes, promover reuniões com fornecedores e grupos de suporte para elaboração do catálogo de serviço técnico, promover reuniões com consumidores para buscar destes informações sobre a intepretação do contrato de serviços.

4.4.6 Recomendação 6: Governança ITIL para SOA

Vimos que podemos fazer uma boa governança SOA a partir dos processos e atividades propostas por ITIL, porém para que tal governança seja feita é necessário que todo o escopo de ITIL e cada aspecto de SOA seja considerado. Seria recomendado para a organização fornecedora de serviços SOA o investimento em conhecimento por parte de seus gestores, da biblioteca ITIL, por meio de cursos e certificações, a utilização de consultores com conhecimento sobre as praticas ITIL também deve ser considerada.

4.4.7 Recomendação 7: Planejar recursos para adequar disponibilidade aos requisitos de mercado

Questões relacionadas à disponibilidade têm sido cada vez mais consideradas nos dias de hoje, uma vez que soluções intolerantes a falhas, como as que funcionam em transações bancárias, têm tido seu tráfego aumentado. SOA por sua vez faz com que a disponibilidade seja um princípio ainda mais discutido, uma vez que indisponibilidade de um único serviço pode fazer com que vários processos tenham sua operação prejudicada.

A fim de que o fornecedor de serviços SOA busque mitigar riscos de disponibilidade, o mesmo deve determinar requisitos de disponibilidade impostas pelo mercado para serviços de TI, e a partir desses estabelecer limites. De posse dos limites, deve ser feito o planejamento para a infraestrutura buscando o uso se componentes robustos e tolerantes a falhas. A duplexação destes como meio de infraestrutura alternativa caso a principal falhe, simular falhas de forma a verificar o funcionamento dos dispositivos, aumentar a capacidade de pessoal por meio de treinamentos.

4.4.8 Recomendação 8: Implementação de segurança da informação em serviços SOA

A implementação de aplicações seguras para SOA é um requisito de estrema relevância, uma vez que um serviço vulnerável irá proliferar suas vulnerabilidades ao longo de soluções que utilize suas funcionalidades. Dessa forma para que um fornecedor de serviços SOA não coloque no mercado serviços vulneráveis e mesmo tenha sua reputação prejudicada, é necessário observância aos princípios de segurança da informação. Um documento com a política de segurança de informação da empresa deve ser produzindo, especificando-se os requisitos de segurança atendidos. Brechas de segurança devem ser buscas e monitoradas por meio de revisões, auditorias e testes de penetração, desenvolvimento proativo de controles de segurança, o acesso ao sistema deve ser totalmente controlado, por meio de controle de direitos e autorizações.

4.4.9 Recomendação 9: Agilizar a produção de serviços SOA, se possível

Em uma transição para SOA, uma empresa cujo princípio seja a produção ágil de software deve ter em mente que a produção de serviços com reuso demanda de tempo e recursos, a ponto de prejudicar a produção ágil. Buscando minimizar os impactos na agilidade de produção a empresa deve elaborar estratégia de transição, descrevendo propostas e objetivos, podendo assim gerenciando a transição, riscos e desvios para a mesma.

Devem ser promovidas reuniões e acordos entre organização (terceiros, parceiros estratégicos, fornecedores e provedores de serviço) e *stakeholders* envolvidos na transição, o reuso de experiência organizacional, *expertise*, ferramentas, conhecimentos e dados históricos relevantes devem ser considerados. Assim como o treinamento e transferências de conhecimentos por meio de cursos para os desenvolvedores de aplicações.

Por fim o reuso de experiências, treinamentos e utilização de padrões de desenvolvimento poderão agilizar a produção de serviços SOA. No entanto é preciso ter em mente que uma plataforma SOA madura não pode ser desenvolvida da noite para o dia, a transição para esta tecnologia de ser planejada e monitorada. Um tempo deve estimado para que a mesma possa começar atingir os requisitos de agilidade necessários ao fornecedor de serviços.

4.4.10 Recomendação 10: Confecção de catálogo de serviços adequado

A visibilidade de um serviço SOA é fundamental para que o mesmo seja percebido, que os usuários conheçam suas funcionalidades e as juguem necessárias para suas soluções.

Um dos riscos associados a SOA está no fato de o princípio da visibilidade ser aplicado somente após a implementação do serviço, alguns detalhes de requisitos e funcionalidades podem passar despercebidos, pelo responsável pela documentação. O ideal é que o próprio desenvolvedor da aplicação no momento em que estiver escrevendo o código do programa, já busque documentar cada uma das partes. Porém na hipótese de o serviço SOA ter que ser documentado após a implementação podemos utilizar as práticas propostas pelo processo de Gerenciamento de Catálogo de Serviço de ITIL.

Durante a produção do Catálogo de Serviço acordos e documentações devem ser feitas entre todas as partes interessadas para as definições do serviço, deve haver o interfaceamento entre fornecedores e grupos de suporte a fim de produção do catálogo de serviço técnico. Encontros com os consumidores devem ser providenciados, a fim de que sejam buscadas destes, informações a respeito a percepção dos mesmos a cerca das funcionalidades do serviço. Dessa forma podem-se planejar melhor as informações contidas no catálogo de serviço e se essas são suficientes para a intepretação por parte dos potenciais usuários.

4.4.11 Recomendação 11: Linguagem de fácil interpretação no catálogo de serviços

Visto que a interpretação do contrato de serviço é primordial pra que um bom serviço SOA tenha chance de reuso, o fornecedor deve buscar a utilização de uma linguagem de fácil entendimento por parte dos potenciais usuários dos serviços. Deve-se considerar o fato de que esses podem não ter o mesmo grau de conhecimento a cerca do desenvolvimento de software daqueles que estão implementando o serviço. A recomendação baseada nos processos de ITIL para utilização de fácil interpretação por parte de pessoas segue a mesma recomendação dada para o princípio da visibilidade no qual um Catálogo de Serviços conciso sobre todos os serviços SOA disponíveis deve ser elaborado.

A fim de se buscar a utilização de linguagem adequada, o gestor deve participar de encontros com fornecedores, grupos de suporte e com usuários a fim de que seja acordada a linguagem, e se a intepretação das informações estão sendo atendidas. Em caso negativo, adequação deve ser feita.

4.4.12 Recomendação 12: Diminuir quantidade de serviços como único ponto de falha

A TI tem se tornado recurso crítico para diversas aplicações, em algumas delas não tolerando a mínima falha, os recursos devem ser contínuos e estar disponíveis sempre que

requisitados. Para garantir que os níveis acordados de continuidade e disponibilidade sejam atingidos deve-se proceder com medidas de redução de riscos e opções de recuperação rápida quando falhas ocorrem. Um único serviço SOA que tiver disponibilidade prejudicada, irá causar impacto em diversas composições de que fizer parte. Buscando minimizar os riscos de falta de disponibilidade e continuidade para composições SOA, trazermos as recomendações baseadas nos processos de Gerenciamento de Disponibilidade e Gerenciamento de Continuidade dos Serviços de TI de ITIL. As recomendações devem ser consideradas em cada um dos serviços membros da composição, para que pontos únicos de falhas sejam minimizados.

Primeiramente o gestor deve determinar requisitos de disponibilidade impostos pelo mercado, para de posse desses possa fazer seu planejamento. Funções vitais para o funcionamento da infraestrutura devem ser listadas e documentadas. A utilização de componentes robustos a prova de falhas deve sempre ser buscada, assim como a duplexação de componentes reservas, utilização de dispositivos de monitoramento para os componentes da infraestrutura e análise das tendências, uso de backup de dados em locais físicos diferentes. Mecanismos de resiliência devem ser projetados, para que a rede seja tolerante a falhas. Por fim, pesquisas com usuários devem ser regularmente feitas para que a satisfação dos mesmos diante dos serviços seja analisada.

4.4.13 Recomendação 13: Dimensionar tempo de resposta de serviços membro de composição

Devido à possibilidade de reuso SOA, podemos combinar funcionalidades de diferentes serviços por meio de composições. Dentre os riscos do uso de diferentes serviços em composições temos o do desempenho, onde um único serviço membro pode prejudicar a eficiência de todo o sistema. O tempo de resposta de cada serviço SOA deve ser avaliado, considerando-se a demanda para o serviço é preciso dimensionar a capacidade de trafego do mesmo.

A recomendação para este risco foi baseada nos processos de Gerenciamento de Demanda e Gerenciamento de Capacidade de ITIL. Dispositivos de monitoramento e medição devem ser instalados em todos os componentes críticos da infraestrutura, análise da tendência na operação de cada um deve ser considerada, buscando-se por gargalos de desempenho, modelagem do sistema para pontos críticos de operação devem ser analisadas. Sempre que possível deve ser feito investimento em melhoria de capacidade para a infraestrutura, otimização deve ser buscada por meio da análise dos resultados de monitoramento dos

componentes, utilização de tecnologias e atualização do gestor para técnicas de uso eficientes dos componentes.

4.4.14 Recomendação 14: Monitoramento e dimensionamento de desempenho de serviço

A fim de se aumentar a independência de Estado de Serviço de serviços SOA, recursos como a delegação para outra parte da arquitetura para a guarda da informação de estados são utilizados. Visto que um número muito grande seções do serviço podem estar atendendo a diferentes chamados ao mesmo tempo, a utilização desse recurso pelo serviço pode exigir maiores requisitos de desempenho para o mesmo, uma vez que parte do processamento será utilizado somente para busca, guarda e interpretação de informações de estado no banco de dados. A fim de monitorar a necessidade de aumento nos recursos para que problemas de desempenho não afetem a operação do serviço, formulamos recomendações baseadas nos processos de Gerenciamento de Capacidade e Gerenciamento de Demanda de ITIL.

O monitoramento, assim como a análise de comportamento para os componentes da infraestrutura de TI devem ser de extrema importância para se verificar a exigência de maior capacidade dos recursos. Modelagens e simulações devem também ser consideradas, a fim de se antever problemas de desempenho na rede. Devem-se estabelecer valores limite de acordo com as observações para o tempo de resposta do banco de dados, tamanho de filas, utilização do disco, taxa de tráfego na rede.

4.5 Resumo das recomendações

Nesta seção listamos todas as recomendações elaboradas com base em ITIL para a segurança de SOA.

1. Controle de versão de serviços SOA;
2. Conhecimento de novas tecnologias;
3. Dimensionamento de desempenho.
4. Conhecer as necessidades dos múltiplos clientes;
5. Catálogo de serviço que proporcione correta interpretação das funcionalidades e requisitos;
6. Governança ITIL para SOA;
7. Planejar recursos para adequar disponibilidade aos requisitos de mercado;

8. Implementação de segurança da informação em serviços SOA;
9. Agilizar a produção de serviços SOA, se possível!;
10. Confecção de catálogo de serviços adequado;
11. Linguagem de fácil interpretação no catálogo de serviços;
12. Diminuir quantidade de serviços como ponto único de falha;
13. Dimensionar tempo de resposta de serviços membro de composição;
14. Monitoramento e dimensionamento de desempenho de serviço;

4.6 Avaliação das recomendações

Todas as recomendações propostas neste trabalho para gestão de riscos de SOA foram elaboradas com base no escopo dos processos de ITIL. Podemos, portanto, fazer uma avaliação do nível de cobertura de ITIL com base na análise das recomendações. Verificando o nível com que cada uma das recomendações tratou os riscos, podemos concluir que todas as recomendações propostas estão em alto nível, ou seja, em um nível estratégico, gerencial.

ITIL se mostrou uma biblioteca bastante ampla, cobrindo os mais diversos tipos de riscos, contudo observamos que ITIL trata de suas soluções sempre a nível estratégico, apontando o que seria a melhor prática para determinados problemas, e dizendo o que fazer, porém nunca indicando como se implementar a solução. Logo uma organização que opte por considerar o escopo de ITIL em suas soluções de TI deve sempre buscar por conhecimento complementar, afim de que consiga implementar as suas propostas.

Verificamos que o fato de ITIL ser bastante amplo e aplicável em diversos cenários, o torna um guia não tão eficiente quanto aplicado no tratamento de cenários particulares, devido às propostas genéricas que o mesmo apresenta. Não descendo ao nível de implementação de TI, ITIL deixa as recomendações com uma aplicação não imediata.

Concluímos que as recomendações propostas neste trabalho podem servir como um guia estratégico para uma organização que estiver iniciando uma implementação SOA. Porém, as mesmas necessitam de uma literatura ou de conhecimentos adicionais para se avaliar a melhor forma de implementar as soluções propostas.

5 Conclusão

A Tecnologia da Informação tem se tornado um componente essencial para os negócios. Cada vez mais atrelado aos negócios têm surgido serviços de TI em que a segurança é característica tão importante quanto à própria funcionalidade. Negócios que não toleram a mínima falha e aplicações das mais diversas que surgem, podem, no caso de incidentes, trazer danos irreparáveis.

No cenário de TI surge SOA- Arquitetura Orientada a Serviços- como uma tecnologia de informação distribuída promissora, cujo ativo principal é o serviço. Dentre os fatos que têm tornado SOA tão aceito, estão suas características de independência de plataforma, linguagem de programação e arquitetura. Dessa forma boa parte do sistema legado de uma organização pode ser aproveitado, mesmo quando grande evolução é observada. O principal artifício, contudo, para o sucesso SOA está na idéia de reuso de serviços. Funcionalidades já implementadas podem facilmente ser incorporadas a novas soluções. SOA é uma tecnologia que agregou todos os resultados de sucesso na história da TI e os incorporou para soluções nos negócios.

Apesar de tantos benefícios observados na implantação de SOA, vários casos de insucesso foram observados em pesquisas conduzidas por revistas do ramo de TI. Tanto nas pesquisas observadas quanto na análise da literatura pudemos observar que questões de gerenciamento e governança SOA estão dentre as principais causas de insucesso em sua implantação. Questões puramente tecnológicas foram responsáveis por poucas causas de fracasso.

SOA representou um cenário próprio para o propósito do nosso projeto, que foi o de propostas de recomendações para segurança baseadas em ITIL. ITIL - *Information Technology Infrastructure Library* – se mostrou um compilado amplo e genérico de boas práticas, aplicáveis nas mais diversas áreas de TI. A biblioteca ITIL , composta por 5 livros, a saber: *Service Strategy, Service Design, Service Transition, Service Operation e Continual Service Improvement,* teve seu escopo formado ao longo da história, decorrido de experiências, *expertise,* e boas práticas conduzidas por influentes da área de TI.

Verificamos na literatura, propostas que conseguiram com sucesso apresentar alternativas para a governança SOA por meio da aplicação dos processos dos ciclos de vida ITIL. Nosso objetivo foi ir um pouco mais além e focarmos em aspectos de segurança, elaborando recomendações baseadas em ITIL para mitigar os riscos associados a SOA.

Dos vinte e cinco (25) processos de ITIL foram necessários onze (11) para cobrir os quatorze (14) riscos associados a SOA considerados no trabalho. Portanto utilizamos 44% do escopo de ITIL para cobrir os riscos considerados.

Verificamos que para os riscos mais ligados a aspectos tecnológicos, a saber: controle de versão, dependências de tecnologia, problemas de desempenho, preocupações com disponibilidade, preocupações com segurança, preocupação com governança, serviço membro de composição como único ponto de falha e membros de composição como gargalo de desempenho, ITIL apresenta recomendações diretas, de alto nível, inclusive indicando soluções de componentes e artifícios tecnológicos que podem ser utilizados. Verificamos que para essas recomendações apesar de considerarmos os riscos mais ligados a aspectos tecnológicos, ITIL não desce no baixo nível, apenas indica as possíveis soluções e não como implementá-las.

Para os riscos ligados a aspectos considerados mais abstratos, a saber: requisitos de acoplamento de múltiplos clientes, interpretação errada pelas pessoas devido ao excesso de abstração, preocupação com desenvolvimento ágil, aplicação do principio da visibilidade após a implementação do serviço e utilização de linguagem de difícil interpretação no contrato de serviço, ITIL permitiu uma análise do escopo dos processos nos possibilitando alinha-los e propor atividades, porém não foram soluções consideradas imediatas, recomendando mais esforço em pesquisas a clientes e fornecedores para entender as necessidades dos mesmos e assim propor soluções.

Concluímos que ITIL serve como um ótimo guia para gestores, iniciarem, manterem e evoluírem suas soluções em TI e, como mostrado pelo nosso trabalho, inclusive com relação a aspectos de segurança. O mesmo cobriu de forma satisfatória os riscos associados a SOA considerados neste trabalho, porém não apresenta nenhuma forma de implementação das recomendações propostas, trabalhando sempre a um nível estratégico.

Para este trabalho esperamos que as propostas de recomendações sejam úteis, funcionando com o um guia inicial para organizações na implantação e gerenciamento seguro de um projeto SOA, baseado em ITIL.

Para trabalhos futuros sugerimos estudos analisando aspectos de segurança em outros guias de referencia como PMBOK, e COBIT também sejam considerados.

Referências bibliográficas

ALCÂNTARA ,R.; SILVA, S. B.; MEDEIROS ,V. C.; GONÇALVES , R.; PUTTINI R.S.; OLIVEIRA , E.C.: **Usando SOA para organizar e acessar informações do RES – RegistroEletrônico de Saúde no Brasil,** UnB;

ARRAJ, Valerie, diretora adminstrativa, Compliance Process Partners, LLC : **ITIL®: The Basics,** White Paper OGC , maio de 2010.

BHALLAMUDI, Pushparani; TILLEY, Scott: **SOA Migration Case Studies and Lessons Learned.**

BIEBERSTEIN, N.: **Executing SOA - A Pratical Guide for the Service- Oriented Architect**, 1. ed., Boston: IBM Press, 2008.

CARTLIDGE, Alison ; HANNA, Ashley ; RUDD, Colin; MACFARLANE, Ivor; WINDEBANK, John ; Stuart RANCE : **AN INTRODUCTORY OVERVIEW OF ITIL® V3**.

CLINCH, Jim, consultor da OGC: **ITIL V3 and Information Security**, white paper OGC maio de 2009.

ERL, Thomas: **SOA Princípios de Design de Serviços**, 2009.

FABER ,Michael; FABER ,Rubina : **ITIL® and Corporate Risk Alignment Guide An introduction to corporate risk and ITIL, and how ITIL supports and is assisted by Management of Risk**, White Paper OGC, 2010;

GHAFAR, Mohammad ; SALEH, Mortaza; MODIRI, Nasser: **A Model to Increase the Trust in Service Oriented Architecture**, 2011 Fifth Asia Modelling Symposium

GRONOSKY, Andrew; ATIGHETCHI, Michael; PAL, Partha: **Understanding the Vulnerabilities of a SOA Platform**, 2010 Ninth IEEE International Symposium on Network Computing and Applications.

HOJAJI, Fazilat; SHIRAZI, M. R. Ayatollazadeh : **Developing a More Comprehensive and Expressive SOA Governance Framework**.

HIGH, R.; KINDER, S.; GRAHAM, S. :**IBM's SOA Foundation - An Architectural Introduction and Overview**, IBM developer Works: IBM's resource for developers and IT professionals, 2005.

HAFNER, M; BREU, R: **Security Engineering for Service-Oriented Architectures,** 2009.

ITILV3 - SERVICE STRATEGY, publicação TSO, 2007.

ITILV3 - SERVICE DESIGN, publicação TSO, 2007.

ITILV3 - SERVICE TRANSITION, publicação TSO, 2007.

ITILV3 - SERVICE OPERATION, publicação TSO, 2007.

ITILV3 - CONTINUAL SERVICE IMPROVEMENT, publicação TSO, 2007

ITILV3- OFFICIAL INTRODUCTION, publicação TSO, 2007

KEEN, M.**: Implementing an SOA Using an Enterprise Service Bus,** IBM RedBooks;

LOWIS, Lutz; ACCORSI, Rafael: **Vulnerability Analysis in SOA-Based Business Processes**, IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 4, NO. 3, JULY-SEPTEMBER 2011.

MCGRAW**,**Gary: **Software Security and SOA:Danger, Will Robinson!**, IEEE SECURITY & PRIVACY, 2006

MÜLLER, I**.: A Conceptual Framework for Unified and Comprehensive SOA Management,** 2009.

OVERBEEK, Paul; CAZEMIER, A. Jacques; PETERS, Louk: **Information Security Management with ITIL v3,** 2009

SUSANTI, Fitri ; SEMBIRING, Jaka : **The Mapping of Interconnected SOA Governance and ITIL v3.0**, 2011 International Conference on Electrical Engineering and Informatics.

XIAN-PENG, Cui; BI-YING, Lin; RUI-FANG, Mo: **An ITIL v3-based Solution to SOA Governance,** 2012 IEEE Asia-Pacific Services Computing Conference.

ZENG, Jihong : **A Case Study on Applying ITIL Availability Management Best Practice**,2008.