Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

No 2 (8)
2009

Sumário

ISSN: 1677-3071

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente. Agora ela volta a ser diagramada em uma única coluna, para facilitar a leitura na tela do computador. Mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

GERENCIAMENTO DE SEGURANÇA SEGUNDO ITIL: UM ESTUDO DE CASO EM UMA ORGANIZAÇÃO INDUSTRIAL DE GRANDE PORTE

SECURITY MANAGEMENT WITH ITIL: A CASE STUDY IN A LARGE INDUSTRIAL ORGANIZATION

(artigo submetido em novembro de 2009)

Vivaldo José Breternitz
Faculdade de Computação e Informática - Universidade Presbiteriana Mackenzie (UPM)
vjbreternitz@mackenzie.br

Francisco Navarro Neto
Faculdade de Computação e Informática - Universidade Presbiteriana Mackenzie (UPM)
fnneto@yahoo.com.br

Alexandre Franco Navarro
Faculdade de Computação e Informática - Universidade Presbiteriana Mackenzie (UPM)
afnavarro@gmail.com

ABSTRACT

In an environment in which organizations increasingly depend on the quality of their information systems to provide services and produce goods in an appropriate manner, it is vital to adopt tools to ensure this quality. One of the most used tools for this purpose is the Information Technology Infrastructure Library (ITIL), in which the module that deals with security management is one of the most important. The objective of this study was to understand how ITIL is used in the process of security management in a large industrial organization, as this understanding may bring useful knowledge to people who are faced with similar situations. This case study was done through semi-structured interviews that allowed the comparison between the ITIL principles to the subject and the practices adopted by the organization object of study.

Key-words: ITIL; information security; IT governance; security management; service level agreement.

RESUMO

Em um ambiente no qual as organizações dependem cada vez mais da qualidade de seus serviços de Tecnologia da Informação para poderem prestar serviços e produzirem bens de forma adequada, torna-se vital adotar ferramentas que garantam essa qualidade. Uma das ferramentas mais utilizadas para esse fim é a biblioteca ITIL (*Information Technology Infrastructure Library*), que possui um módulo que trata de gerenciamento da segurança. O objetivo da pesquisa apresentada neste trabalho foi compreender a forma pela qual a ITIL é utilizada no processo de gerenciamento de segurança na área de TI de uma organização industrial de grande porte, o que pode gerar conhecimentos úteis aos que venham a atuar em situações similares. Essa compreensão foi obtida por meio de um estudo de caso, realizado com aplicação de entrevistas semiestruturadas que permitiram a comparação entre as propostas de ITIL para o tema e as práticas adotadas pela organização objeto do estudo.

Palavras-chave: ITIL; segurança da informação; governança de TI; gerenciamento de segurança; acordo de nível de serviço.

1 INTRODUÇÃO

Atualmente a qualidade de produtos e serviços é um grande diferencial para as organizações, em um ambiente em que a concorrência entre elas é cada vez mais acirrada. A qualidade deve estar presente em todas as fases dos processos produtivos, uma vez que um produto ou serviço integralmente desenvolvido com qualidade, além de agregar valor ao cliente, evita perdas para o fornecedor.

Outra constante no cotidiano das organizações é o valor que as informações agregam ao negócio. Essas informações vão desde procedimentos internos da organização e dados de seus sistemas transacionais até segredos de negócio e informações sigilosas de clientes. Nesse ambiente, é vital a adoção de medidas que possam garantir a segurança das informações ou, ao menos, reduzir a possibilidade de sinistros.

Dentre essas medidas, está a implementação de uma governança de TI eficaz, entendida como um conjunto de mecanismos que estimulam comportamentos consistentes com a missão, a estratégia, os valores, as normas e a cultura da organização (WEILL; ROSS, 2006).

Uma das ferramentas que pode ser utilizada para a prática da governança de TI é a ITIL (*Information Technology Infrastructure Library*), uma biblioteca de melhores práticas de governança de TI, frequentemente citada como um dos mais populares *frameworks* para governança de TI (RUDD, 2004). A utilização da ITIL vem crescendo nos últimos anos, em decorrência não apenas do aumento da demanda por governança de TI, como também da evolução da própria ITIL, que já está em sua terceira versão.

Nesses termos, o objetivo da pesquisa aqui relatada foi compreender a forma pela qual a ITIL é utilizada no processo de gerenciamento de segurança na área de TI de uma organização industrial de grande porte, que no âmbito deste trabalho será chamada *organização*. Essa compreensão pode gerar conhecimentos úteis aos que venham a atuar em situações similares.

2 ASPECTOS METODOLÓGICOS

Este trabalho apresenta os resultados de uma pesquisa exploratória qualitativa, desenvolvida com base em um estudo de caso.

Selltiz *et al.* (1987) dizem que a pesquisa exploratória proporciona maior familiaridade com o problema, com vista a torná-lo mais explícito ou construir hipóteses para posterior investigação mais profunda, tendo como objetivo também aprimorar ideias e despertar intuições. Na maioria dos casos, isso envolve levantamentos bibliográficos, entrevistas com pessoas que tiveram experiências práticas com o problema e análise de exemplos que estimulem a compreensão do assunto.

Na pesquisa relativa ao objeto desse trabalho a opção foi por uma abordagem qualitativa. Assim, as perguntas elaboradas não possibilitam respostas mensuráveis, na maioria das vezes, e, quando são mensuráveis, não o são de forma precisa. Mattar (2001) e Malhotra (2008) afirmam que, em situações como essa, considerar apenas a pesquisa quantitativa pode levar a resultados muito superficiais e talvez incorretos.

Miles (1979) afirma que o enfoque qualitativo tem obtido crescente popularidade na pesquisa organizacional, pelo seu caráter rico, holístico e "real". Segundo Malhotra (2008), a abordagem qualitativa proporciona melhor visão e compreensão do contexto do problema, de modo que, ao se abordar um novo problema, a pesquisa quantitativa deve ser precedida de pesquisa qualitativa apropriada. Miles e Huberman (1994) consideram que a pesquisa qualitativa leva a um contato intenso com o objeto sob estudo, o que acaba produzindo um conhecimento mais profundo dele.

Cabe ressaltar que as estratégias de pesquisa quantitativa e as de pesquisa qualitativa não são mutuamente excludentes. Estudos futuros do objeto de pesquisa desse trabalho podem vir a exigir a adoção de procedimentos quantitativos.

Mattar (2001) afirma que o estudo de casos é um método muito produtivo para estimular a compreensão e ampliar os conhecimentos sobre o problema em estudo. Diz também não existirem regras para a escolha dos casos a serem trabalhados e que a experiência mostra que casos que refletem situações extremas podem ser de melhor aproveitamento, talvez ajudando a estabelecer padrões ou estereótipos que podem não ser totalmente indesejáveis. Na visão desse autor, no estudo de casos "médios", pode-se conseguir enxergar apenas pequenas diferenças, tornando a pesquisa menos útil.

Yin (2005), ao comparar o estudo de caso com outros métodos como experimento, *survey* etc., diz que essa estratégia de pesquisa é a mais indicada para responder a questões do tipo "como" e "por que", especialmente quando o pesquisador não tem controle sobre o comportamento dos eventos.

Nesses termos, justifica-se a escolha, como objeto da pesquisa, de uma organização industrial de grande porte, com uma área de TI atendendo a problemas complexos. Foram realizadas no primeiro semestre de 2009 entrevistas semi-estruturadas com seis profissionais da área de TI dessa empresa, em nível de gerência, tendo o resultado da análise dos dados coletados passado por um processo de validação junto a eles.

O roteiro das entrevistas abordou além dos processos relativos à segurança de informação temas como o alinhamento estratégico entre TI e negócios, gerenciamento de risco, governança de TI etc. O roteiro básico das entrevistas compreendeu os pontos que se seguem:

- Razões da adoção de ITIL
- Importância atribuída pela organização aos ativos de TI
- Situação anterior à implementação de ITIL
- Duração do processo de implementação

- Ordem de implementação das diversas disciplinas
- Profissionais responsáveis pela implementação
- Problemas encontrados
- Situação atual em termos de estrutura e procedimentos formais, métricas
- Utilização de ferramentas de *software* nas atividades rotineiras ligadas a ITIL
- Forma de utilização do gerenciamento de segurança
- Aspectos ligados a auditoria
- Percepção dos envolvidos quanto à efetiva utilidade de ITIL para a organização e sobre o nível de aderência às práticas ITIL

Não houve autorização para gravação das entrevistas. Imediatamente após a realização, de cada uma, as notas tomadas pelos pesquisadores eram complementadas, com o objetivo de reter o maior volume de dados possível. Concluídas as entrevistas, foram os dados organizados, servindo de base para discussão e análise entre os pesquisadores, onde se procurou identificar os aspectos relevantes, que poderiam atender aos objetivos da pesquisa. Em alguns casos, quando se julgou necessário esclarecer pontos específicos, os entrevistados foram contatados novamente, por telefone ou correio eletrônico; concluído o processo de análise, foram as conclusões submetidas aos entrevistados para validação.

3 FUNDAMENTAÇÃO TEÓRICA

Esta seção tem como objetivo apresentar os principais conceitos acerca dos temas centrais deste trabalho: segurança da informação e riscos, governança de TI e ITIL.

3.1 SEGURANÇA DA INFORMAÇÃO E RISCOS

No passado, as preocupações com segurança da informação restringiam-se praticamente à integridade das instalações de processamento de dados e à possibilidade de prejuízos financeiros em função de fraudes, estas últimas basicamente no âmbito das instituições financeiras. Mais recentemente, este contexto se expandiu. Após a lei Sarbanes-Oxley, o paradigma de segurança alterou-se, de forma que manter o controle dos processos de segurança tornou-se uma tarefa crucial, porque tais processos afetam diretamente o negócio (BLOEM; VAN DOORN; MITTAL, 2006).

A segurança de informação é implementada por meio de planos de segurança, que devem contemplar os processos de toda a organização. Segundo Bishop (2003), a implantação destes planos envolve:

- *requisitos de segurança*: as necessidades de segurança variam de uma organização para outra. Uma pequena oficina mecânica certamente não possui os mesmos requisitos de segurança de um banco. Estes requisitos devem ser determinados pela organização com a ajuda de uma equipe de *segurança da informação* e devem ser

claros e específicos, pois serão a base de toda a política de segurança. Eles devem ser analisados em profundidade, porque diferentes sistemas podem ter requisitos de segurança distintos dentro de uma mesma organização;

- *política de segurança*, que estabelece as regras de segurança da organização. Basicamente, é expressa em um documento que define os comportamentos desejáveis dos sistemas e usuários de TI de uma organização. Quando o sistema opera de acordo com a política, pode-se dizer que o sistema é seguro (caso contrário, não, e medidas devem ser tomadas para se corrigir a situação);
- *mecanismos de segurança*: garantem que a política de segurança será seguida dentro da organização. Estes mecanismos podem ser técnicos, como a utilização de *firewalls*, ou burocráticos, como penalidades àqueles que desobedecerem a uma determinada regra. O importante é que esses mecanismos, unidos, sejam vistos como uma política de segurança a ser aplicada em toda a organização; e
- *avaliações de segurança*: consistem em certificar-se de que os requisitos, políticas e mecanismos de segurança existentes estão sendo seguidos e ainda se encontram de acordo com as necessidades do negócio, gerando informações para alterações, quando for o caso.

Além dos problemas de natureza humana, com as pessoas frequentemente negligenciando aspectos relativos à segurança, por considerá-los pouco importantes e geradores de custos e de trabalhos adicionais, há que se lembrar que, no caso de sistemas de informações baseados em computadores, há aspectos peculiares a serem considerados, dentre os quais o fato desses sistemas serem, como diz Schneier (2001):

- complexos: pois possuem diversos componentes internos, cuja relação poucas vezes é inteiramente conhecida, ou seja, uma falha em um destes componentes pode gerar resultados inesperados em outro;
- interativos: os sistemas se relacionam entre si, o que aumenta ainda mais sua complexidade e torna pouco eficaz a verificação isolada de um único sistema;
- emergentes: devido à interatividade, os sistemas assumem características não projetadas originalmente, adquirindo novas funcionalidades, como por exemplo, as capacidades de multimídia integradas à Internet; e, principalmente,
- falíveis: os sistemas usualmente possuem falhas de concepção, projeto e construção, e muitas destas acabam por causar ameaças de segurança. A correção destas falhas deve levar em consideração os fatores anteriormente descritos, o que torna esse processo ainda mais complexo.

Esses aspectos mostram o quanto é difícil administrar o assunto *segurança da informação*, e que garantir 100% de segurança em qualquer sistema é uma tarefa árdua, quase impossível, pois a segurança envolve tantos aspectos que por mais que se adotem meios de defesa, ainda existirão vulnerabilidades impedindo que o sistema seja totalmente seguro.

Assim sendo, pode-se dizer que a busca pela segurança de TI é, na prática, o gerenciamento do risco representado pela perda, indisponibilidade temporária ou mau uso da informação (WINKLER, 2007). *Gerenciamento de risco*, segundo Kerzner (2003), pode ser entendido como o ato de lidar com o risco. Inclui atividades como avaliar a probabilidade da ocorrência de sinistros, desenvolver estratégias para lidar com o risco e monitorar os riscos para determinar como eles evoluem.

Observa-se então que para o processo de segurança ser eficiente, deve ser acompanhado de perto pela alta administração da organização. Afinal, são os interesses maiores do negócio que devem ditar as reais necessidades e prioridades da segurança. A fim de obter a devida atenção dos altos níveis da organização, deve-se criar um modelo de gestão que deixe clara a necessidade do acompanhamento desse processo em todos os níveis, e uma boa maneira para se chegar a tal modelo é por meio da governança de TI.

3.2 GOVERNANÇA DE TI

De acordo com Weill e Ross (2006, p. 2), a governança de TI pode ser considerada “a especificação dos direitos decisórios e do *framework* de responsabilidades para estimular comportamentos desejáveis na utilização da TI”. Dentre esses direitos decisórios estão os relativos ao papel estratégico que a TI exerce no ambiente de negócios, a arquitetura adequada, a infraestrutura, os processos operacionais, os investimentos etc.

Esses mesmos autores lembram que os ativos de TI estão entre os principais ativos de uma organização, devendo por essa razão ser objeto de especial atenção no contexto da governança corporativa, para que possam criar valor para a organização.

Para que se crie valor, deve-se procurar minimizar as possibilidades de ocorrência de falhas que gerem riscos no ambiente de TI. Uma das formas de se fazer isso é pela utilização da disciplina *gerenciamento de segurança*, que está contida na ITIL, que é um dos mais utilizados *frameworks* para implementação da governança de TI, como já se disse (RUDD, 2004).

3.3 ITIL

A biblioteca ITIL foi desenvolvida por órgãos do governo britânico no final da década de 1980 e tem como foco principal a operação e a gestão da infraestrutura de TI na organização, incluindo todos os pontos importantes no fornecimento dos serviços prestados pela área (OGC, 2004).

A ITIL descreve os processos que são necessários para dar suporte adequado à utilização e ao gerenciamento da infraestrutura de TI, levando em conta também os custos envolvidos, de forma que se possa perceber como estes trazem valor estratégico ao negócio. Em meados de 2007, foi lançada sua versão 3.0, composta por cinco livros, cujo conteúdo é basicamente o que se segue:

- *Estratégia de serviços:* esse livro aborda principalmente as estratégias, políticas e restrições sobre os serviços. Inclui também temas como implementação, redes de valor, portfólio de serviços, gerenciamento, gestão financeira e ROI (*return on investment* - retorno do investimento);
- *Design de serviços:* nesse livro são tratadas políticas, planejamento e implementação. É baseado nos cinco aspectos principais de design de serviços: disponibilidade, capacidade, continuidade, gerenciamento de nível de serviço e *outsourcing*. Também estão presentes informações sobre gerenciamento de fornecedores e de segurança da informação;
- *Transição de serviços:* apresenta conceitos sobre o sistema de gerenciamento do conhecimento dos serviços. Também aborda mudanças, riscos e garantia de qualidade. Os processos tratados, entre outros, são planejamento e suporte, gerenciamento de mudanças, gerenciamento de ativos e configurações;
- *Operações de serviços:* operações cotidianas de suporte é o foco desse livro, que trata do gerenciamento de *service desk*, requisições de serviços, gerenciamento de incidentes e de problemas, etc.;
- *Melhoria contínua de serviços:* a ênfase do livro está no ciclo "planejar, fazer, verificar e agir", de forma a buscar a melhoria contínua dos processos detalhados nos quatro livros anteriores, visando a aprimorar os serviços prestados aos clientes e usuários.

Com o lançamento da versão 3.0, procurou-se eliminar redundâncias encontradas nos diversos livros, tornando mais clara e forte a ligação entre as melhores práticas e os benefícios para o negócio. Essa versão tem uma abordagem baseada no ciclo de vida, ao contrário da abordagem baseada em setores de entrega da versão anterior.

Apesar de já haver sido lançada a versão 3.0, a organização que foi objeto desta pesquisa ainda utiliza a versão 2, que é composta por sete livros, a saber:

- *Suporte a serviços:* abrange os processos voltados ao suporte do dia-a-dia e às atividades para a sua manutenção;
- *Entrega de serviços:* é voltado aos processos de planejamento e entrega dos serviços de TI, preocupando-se em garantir um alto nível de qualidade a esses serviços;

- *Planejamento para implementar o gerenciamento de serviços de TI:* especifica os passos necessários para identificar como uma organização pode alcançar e usufruir os benefícios da ITIL;
- *Gerenciamento da infraestrutura de TI e telecomunicações:* aborda os processos, organização e ferramentas necessários ao fornecimento de uma infraestrutura estável de TI e comunicações;
- *Gerenciamento de aplicações:* é um guia para o gerenciamento das aplicações partindo das necessidades do negócio, passando por todos os estágios do ciclo de vida de uma aplicação. Este processo dá ênfase a assegurar que os projetos de TI e as estratégias estejam corretamente alinhados com o ciclo de vida da aplicação, garantindo que o negócio consiga obter o retorno do valor investido;
- *Perspectiva de negócios:* auxilia os responsáveis por TI a entenderem como podem contribuir da melhor forma para os objetivos do negócio da organização, além de demonstrar como as suas funções e serviços podem ser alinhados e aproveitados na organização; e
- *Gerenciamento de segurança:* este livro, foco deste trabalho, detalha o processo de planejamento e gerenciamento da segurança da informação e serviços em TI.

Em virtude do advento da versão 3.0, que tende a substituir a versão 2, será considerado aqui apenas o livro que discute o gerenciamento da segurança, por ainda estar em uso na organização.

Segundo o OGC (2004), “o gerenciamento de segurança é uma disciplina que gerencia o nível de segurança da informação definido sobre os serviços de TI”. Ele é o responsável por manter o controle sobre os possíveis incidentes de segurança que possam vir a causar danos em termos de confidencialidade, integridade e disponibilidade da informação, medindo o seu risco e impacto sobre o negócio. Essa disciplina tem origem em uma norma britânica para gestão de segurança de informação, a BS7799, criada em 1995 e que evoluiu até 1999, quando se transformou na norma ISO/IEC 17799:2000.

O *gerenciamento de segurança* interage continuamente com as diversas disciplinas da ITIL, em todos os níveis organizacionais (estratégico, tático e operacional), como ilustrado na Figura 1 (OGC, 2004). Em termos de ambiente de TI, diz-se geralmente que o *gerenciamento de segurança* usualmente está posicionado no nível tático, nos termos usualmente utilizados em que se considera terem as organizações três níveis: estratégico, tático e operacional.

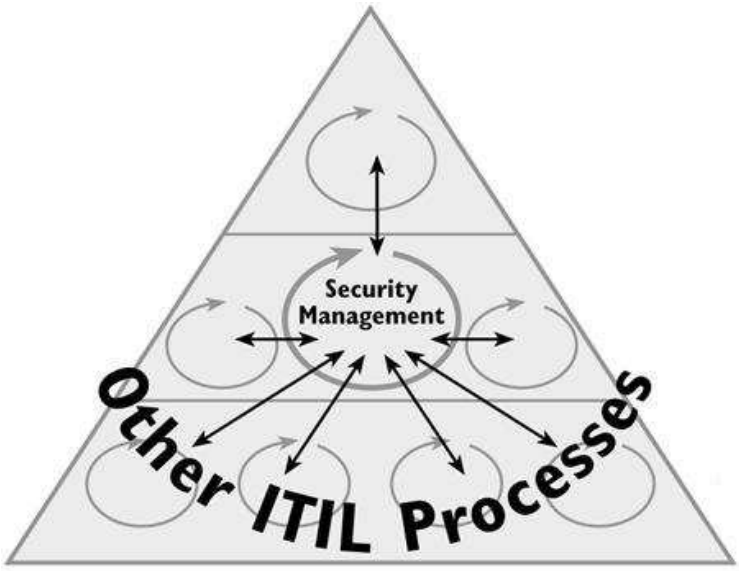

Figura 1 – Gerenciamento de Segurança e a dependência entre as disciplinas
Fonte: OGC (2004)

No nível estratégico, o *gerenciamento de segurança* se compromete a fornecer as informações necessárias para o entendimento da alta administração a respeito das atividades relacionadas à segurança de informação necessária aos negócios: novas políticas de segurança, seu grau de importância e definição das medidas serão tomadas para conter o risco de uma eventual perda de informação, relacionada a incidentes de segurança, caso o risco esteja definido dentro de uma política (OGC, 2004).

No nível tático, o *gerenciamento de segurança* se baseia em Acordos do Nível de Serviço (SLA – *Service Level Agreements*) celebrados entre a área de TI e as áreas clientes. Em função dos níveis acordados, são criados planos de segurança e definidas as políticas necessárias para suportar a demanda de informação gerada pelo negócio.

No nível operacional são aplicadas as políticas definidas no nível tático. Isto assegura o gerenciamento operacional sobre os recursos de TI (OGC, 2004).

O OGC (2004) divide os requisitos de segurança em dois grandes grupos: requisitos externos (aqueles derivados de contratos, legislação e outros fatores externos à organização) e requisitos internos (relacionados aos acordos de nível de serviço celebrados com os gestores dos sistemas).

Esses requisitos levam à geração de planos de segurança, que, de acordo com ITIL, são documentos gerados pelo gerente de segurança. Esses documentos devem conter a situação atual da organização, metas específicas a serem cumpridas e a situação almejada no futuro. Definem ainda as prioridades para o bom andamento dos negócios, seus responsáveis e demais envolvidos, além dos desafios e de como contorná-los, a fim de manter o nível de serviço em um padrão aceitável.

A Figura 2, adaptada de OGC (2004) mostra de forma esquemática como a ITIL vê o processo de *gerenciamento de segurança*:

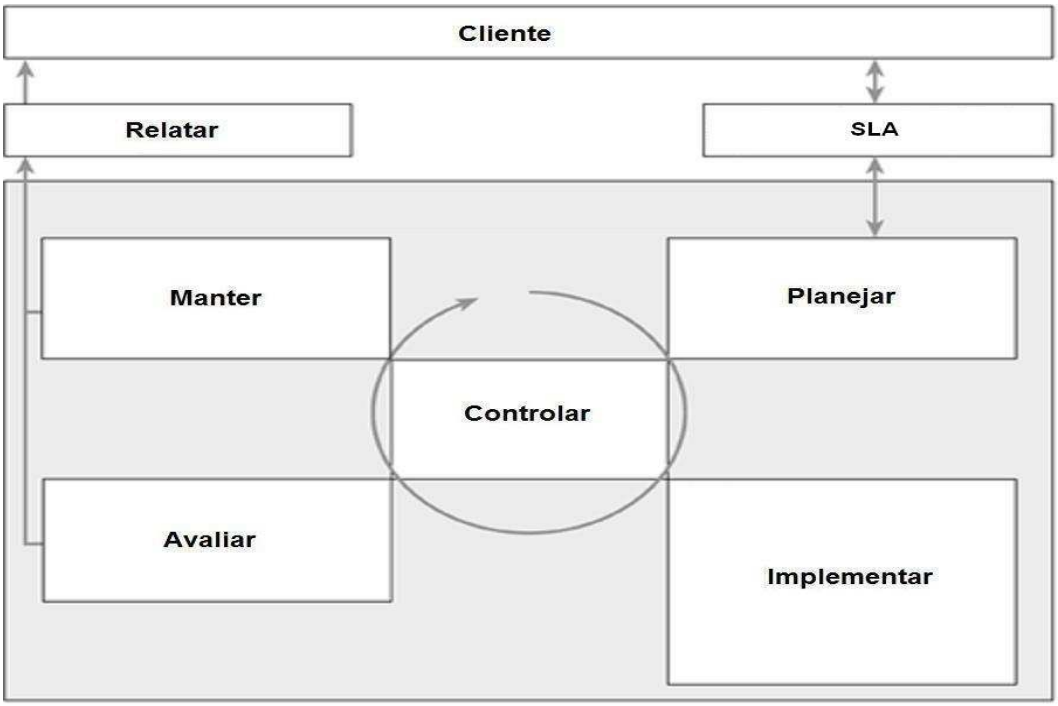

Figura 2 - Processo de Gerenciamento de Segurança
Fonte: adaptado de OGC (2004)

De maneira resumida, as atividades que compõem esse processo podem ser descritas como se segue:

- *Planejar*: busca garantir que o nível de segurança foi estabelecido e definido em conjunto com o cliente, de forma a atender as suas expectativas. Aqui também são definidos políticas, regras, medidas e manuais de segurança para orientar os envolvidos;
- *Implementar*: esta atividade tem como objetivo por em prática as ações planejadas anteriormente;
- *Avaliar*: compreende a realização de auditorias internas e externas no ambiente, revisando políticas e medidas de segurança, com o objetivo de descobrir se estão sendo aplicadas corretamente. Esta atividade garante que o ambiente não foi modificado, permitindo continuar a cumprir os acordos de SLA pré-estabelecidos. As ameaças identificadas serão reportadas e analisadas, visando a evitá-las ou minimizá-las;
- *Manter*: esta atividade atualiza os acordos de SLA e as medidas e planos de segurança existentes, melhorando-os para que possam garantir a manutenção e melhoria de qualidade;
- *Controlar*: é a atividade integradora, que garante que o que foi planejado será executado;
- *Relatar*: esta atividade é de grande importância para os usuários, pois os mantém informados sobre a situação do ambiente de segurança de TI. Baseia-se principalmente nos resultados das auditorias e nos indicadores de desempenho do ambiente.

O processo de *gerenciamento de segurança* começa pelo contato com o cliente, quando se elabora o SLA e se definem suas necessidades. O processo se repete em um ciclo de retroalimentação e tem como objetivo revisar as políticas e planos de segurança a fim de encontrar seus pontos fracos e detectar mudanças no ambiente que possam trazer ameaças à segurança.

De acordo com Tipton e Krause (2008), este processo pode ser comparado com o Círculo da Qualidade de Deming, que tem como atividades planejar, fazer, verificar e agir, sempre com a finalidade de aperfeiçoar o processo, garantindo uma melhora na qualidade do serviço fornecido.

4 APRESENTAÇÃO DO CASO

A organização objeto desta pesquisa é a operação brasileira de uma indústria automobilística, uma montadora de grande porte de origem estrangeira, com mais de 250 mil empregados no mundo. Sua primeira fábrica no Brasil foi aberta em 1930.

Sua área de TI no Brasil conta com cerca de 50 empregados diretos e cerca de 2.500 terceirizados. Os empregados diretos ocupam cargos de gerência e auditoria. Os gerentes usualmente são considerados pontos focais - ou clientes - dos prestadores de serviços terceirizados e estão distribuídos de acordo com as linhas de serviço da área de TI, como manufatura, sistemas de negócio, redes lógica e física, correio eletrônico etc. Os auditores estão organizados de forma similar, sendo o foco de seu trabalho a verificação do trabalho executado pelos prestadores de serviço de TI.

A organização adotou ITIL por considerar este um padrão internacional de boas práticas consagrado e por ter conseguido trazer os retornos esperados em diversas outras organizações. O processo de implantação iniciou-se há cerca de dez anos. Primeiramente foi implementada a disciplina central de serviços e incidentes, e a seguir gerenciamento de problemas, mudanças, configuração, liberação etc. O processo foi conduzido por uma prestadora de serviços na área de TI, uma empresa de grande porte com forte presença no cenário internacional.

No início da implantação de ITIL, houve alguns problemas relacionados à adaptação dos usuários e equipes de TI aos novos processos. Hoje esses problemas estão resolvidos e a maioria dos usuários tem a compreensão de como funcionam os processos da área de TI.

Atualmente, a organização se utiliza de ferramentas de *software* adquiridas no mercado ou desenvolvidas internamente para a operacionalização das disciplinas da ITIL. Dentre estas, pode-se citar ferramentas para controle de incidentes, itens de configuração, problemas, mudanças etc. O uso dessas ferramentas permite a obtenção de relatórios concisos e relevantes, que informam de forma concreta a situação da área de TI, apoiando assim o processo de tomada de decisão por parte da alta

administração, além de decisões no nível tático. O conteúdo desses relatórios foi definido pela organização, com o apoio da prestadora de serviços que atua no processo de implementação. Cabe registrar que se apurou que a alta administração considera os ativos de TI como estratégicos para o seu sucesso, tomando decisões de investimentos baseadas principalmente no retorno que será proporcionado por estes.

Antes da implementação de ITIL, os procedimentos de segurança utilizados eram dispersos e não padronizados, distribuídos entre as diversas linhas de serviços e regiões geográficas em que estão situadas as dependências da organização. A necessidade de padronização e a importância de se gerenciar estes procedimentos levaram à adoção de ITIL. A organização ainda não concluiu a instalação do *gerenciamento de segurança* centralizado, sendo este distribuído de acordo com as linhas de serviço de TI da empresa, embora seus processos já apresentem certo grau de integração.

O *gerenciamento de segurança* atua de forma a balizar os processos das demais disciplinas, mais especificamente *gerenciamento de mudanças, de incidentes, de problemas* e *liberação.* Sempre que um novo requisito de negócio é determinado, é analisado sob a ótica do *gerenciamento de segurança*. Um exemplo disso: sempre que há necessidade de mudança de *software* ou *hardware*, o *gerenciamento de liberação* repassa essa necessidade ao *gerenciamento de segurança*, onde especialistas verificam a melhor forma de liberar essas novas versões aos usuários. As mudanças então são documentadas, de forma a se estabelecer um processo para a sua implantação em toda a organização e, a partir de então, são criados os registros de mudanças delas derivados.

Os incidentes de segurança são relatados a uma central de serviços, que resolve os casos mais simples. Os demais são encaminhados às equipes de especialistas que discutem a melhor forma para solucionar o problema, buscando minimizar o impacto sobre os usuários.

A organização possui métricas específicas para se determinar rapidamente o impacto de incidentes de segurança, que levam em consideração o tempo de parada, a criticidade do sistema, o número de usuários afetados etc. O cálculo deste impacto varia de acordo com a linha de serviços de TI (no jargão da organização, a expressão “linha de serviços” significa o conjunto de serviços prestados a uma de suas áreas).

Desde o momento em que um incidente é comunicado, este é registrado em um sistema próprio, o que também ocorre com todas as providências tomadas até que a ocorrência esteja solucionada e validada pelo usuário para seu encerramento (análise *end-to-end*). Depois de encerrado seu tratamento, o incidente continua registrado no sistema, pois com essa informação são definidos possíveis pontos de melhoria nos processos e geradas métricas de desempenho da área de TI para a organização.

A organização procura evitar incidentes de segurança tomando medidas pró-ativas de verificação de segurança nos procedimentos adotados

no ambiente, o que envolve verificar se esses procedimentos podem, de alguma forma, constituir ameaça à organização. Os incidentes também são evitados por meio da constante atualização dos sistemas operacionais, antivírus e demais ferramentas de *software,* de acordo com o estabelecido pelos seus fornecedores. Reativamente, a organização se utiliza de lições aprendidas com incidentes passados, tomando as devidas medidas para que não voltem a ocorrer.

Na organização, os requisitos de segurança são aplicados por meio de planos de segurança, que variam de acordo com a linha de serviços de TI. Esses planos agregam valor aos serviços prestados pela área de TI da organização, pois por meio deles se assegura que os usuários de uma determinada linha recebam um serviço padronizado e que tenham a compreensão de como utilizar seus recursos da melhor forma.

Os planos são vistos na prática como regulamentações de uso de ativos de TI, normas internas para gerenciamento do ambiente, programas de conscientização de funcionários para as políticas da organização e até mesmo como regras para a aplicação de sanções para os infratores.

Para criar os planos de segurança, os gerentes de TI de uma determinada linha de serviços partem de uma necessidade pontual para a segurança dos ativos de TI, verificando junto às equipes responsáveis os meios, tecnológicos ou não, que possam ser empregados para esse fim. Essas mesmas equipes ajudam a avaliar o impacto dessas medidas no ambiente e, concluída a análise, colocam as medidas em prática. Depois de o plano ser colocado em prática, ele é revisado periodicamente para que se possa avaliar sua eficácia e, caso necessário, são propostas mudanças com a finalidade de melhor atender às necessidades do negócio.

Dentre essas equipes de apoio, pode-se ressaltar as equipes das prestadoras de serviços como conselheiras em tecnologia e as equipes de recursos humanos e da gerência das áreas interessadas como conselheiros não tecnológicos.

Os planos contêm as medidas a serem adotadas, o que se espera com sua adoção, a forma de medição da sua eficácia e quem é responsável por prover essas métricas. O ambiente é auditado externa e internamente ao menos uma vez por ano, sendo que alguns sistemas mais críticos são auditados mais frequentemente.

A organização não possui uma área específica para o gerenciamento de risco, deixando aos gerentes de TI a responsabilidade pelos riscos de suas respectivas linhas de serviço, o que torna a organização de alguma maneira ciente dos riscos a que está sujeita. A postura da organização perante os riscos é, de certa forma, conservadora, preferindo evitar riscos sempre que possível, embora essa postura mude de acordo com a linha de serviços de TI.

Como não existe o gerenciamento de risco formal, não existe um registro dos riscos de TI, este sendo substituído pela base de dados de incidentes em uso pela organização, de onde são retiradas informações para a prevenção de incidentes futuros.

Com a inexistência do registro de riscos, a análise de riscos também ocorre de forma relativamente informal, baseando-se quase que totalmente na vivência dos prestadores de serviço mais experientes, que conhecem o ambiente de forma a antecipar as possíveis ameaças facilmente.

5 CONSIDERAÇÕES FINAIS

Apresentados os procedimentos adotados pela organização, conclui-se agora com uma comparação entre estes e os processos de segurança recomendados por ITIL.

Verifica-se que a área de TI da organização realmente leva em consideração os objetivos do negócio para definir como melhor utilizar seus recursos. Esse alinhamento entre TI e o negócio é confirmado pela percepção dos entrevistados no sentido de que a alta administração tem confiança nas informações geradas pela área através dos processos ITIL.

Percebe-se que a ITIL serve de sustentação para os processos de segurança utilizados pela organização, embora diferenças entre o prescrito e o adotado no âmbito do gerenciamento de segurança sejam notadas. Dentre essas diferenças, destacam-se a falta de papéis mais claros para a gerência de segurança e a descentralização dos processos de gerenciamento de segurança, que resultam em políticas não totalmente padronizadas.

No que se refere ao processo de elaboração de planos de segurança, conclui-se que a organização adota algumas das práticas ITIL, pois nota-se o envolvimento consciente de seus membros durante o desenvolvimento destes planos, bem como a retroalimentação do processo com o intuito de incrementar sua qualidade.

Com relação ao gerenciamento de riscos, fica claro que há ainda muito a se fazer para que os riscos sejam enfrentados de forma eficiente, embora essa necessidade seja aplacada em parte pelos processos do gerenciamento de segurança.

Pode-se concluir também que o ambiente estudado não está totalmente de acordo com o proposto por ITIL, que em teoria foi a base de sua estruturação. Os envolvidos têm a percepção de que as necessidades do negócio são atendidas, embora a situação ainda possa ser melhorada.

Para melhoria, sugere-se que o processo de gerenciamento de segurança na organização seja centralizado e formalizado, assumindo os poderes e responsabilidades necessários a um gerenciamento de segurança eficiente.

Ainda é necessário um gerenciamento de risco formal, estabelecendo responsabilidades e delegando autoridade suficiente para que se possa lidar com os riscos de forma mais eficaz, pois somente com esta formalização a organização poderá compreender e lidar adequadamente com os riscos a que está sujeita.

Para trabalhos futuros a respeito do gerenciamento de segurança em ITIL, sugere-se um estudo comparativo entre as versões 2 (antiga) e 3 (atual), com foco nas vantagens da nova versão sobre a antiga, bem como em eventuais dificuldades para a migração para a versão 3. Acredita-se que esse estudo possa gerar conhecimentos úteis aos que venham a atuar em processo de migração da versão 2 para a versão 3.

REFERÊNCIAS

BISHOP, Matt. What is computer security? *IEEE Security & Privacy,* Los Alamitos, v. 1, n. 1, p. 67-69, Jan./Feb. 2003.

BLOEM, Jaap; VAN DOORN, Menno; MITTAL, Piyush. *Making IT Governance work in a Sarbanes-Oxley world*. Hoboken: John Wiley & Sons, 2006.

KERZNER, Harold. *Project Management:* a systems approach to planning, scheduling, and controlling. Hoboken: John Wiley & Sons, 2003.

MALHOTRA, Naresh K. *Pesquisa de marketing:* uma orientação aplicada. Porto Alegre: Bookman, 2008.

MATTAR, Fauze N. *Pesquisa de marketing.* São Paulo: Atlas, 2001.

MILES, Matthew B. Qualitative data as an attractive nuisance: the problem of analysis. *Administrative Science Quarterly,* Ithaca, v. 24, n. 4, p. 590-601, Dec. 1979.

MILES, Matthew B; HUBERMAN, A. Michael. *Qualitative data analysis:* an expanded sourcebook. Thousand Oaks: Sage, 1994.

OGC. *ITIL Security Management.* Londres: The Stationary Office, v. 1.0, 2004.

RUDD, Colin. An introductory overview of ITIL. Webbs Court (UK): iTSMF, 2004. Disponível em http://www.paradigm-itsm.com/documents/ITIL_Overview_Book-itSMF.pdf. Acesso em: 27/06/2008.

SCHNEIER, Bruce. *Segurança.com:* segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001.

SELLTIZ, Claire; WRINGHTSMAN, Lawrence S.; COOK, Stuart. *Métodos de pesquisa nas relações sociais:* delineamento de pesquisa. São Paulo: EPU, 1987.

TIPTON, Harold F.; KRAUSE, Micki. *Information Security Management Handbook.* 6. ed., vol. 2. Boca Raton: Auerbach, 2008.

WEILL, Peter; ROSS, Jeanne W. *Governança de TI: tecnologia da informação.* São Paulo: Makron Books, 2006.

WINKLER, Ira. *Zen and the art of information security.* Rockland: Syngress, 2007.

YIN, Robert.K. *Estudo de caso* – planejamento e métodos. Porto Alegre: Bookman, 2005.