5CONTECSI June 04 - 06, 2008 São Paulo, Brazil

5th International Conference on Information Systems and Technology Management
5º Congresso Internacional de Gestão da Tecnologia e Sistema de Informação
De 04 a 06 de Junho de 2008 - São Paulo - Brasil

PS-1108

ITIL ON SECURITY INFORMATION MANAGEMENT

Rogério Mendes (UNIPAC – Universidade Presidente Antônio Carlos, Minas Gerais, Brasil) - rogerio@websec.com.br
Marcio Aurélio Ribeiro Moreira (UNIMINAS – União Educacional Minas Gerais, Minas Gerais, Brasil) - marcio.moreira@uniminas.br

The security information, since its principle aimed at to all assures the control and the access of the systems/users and the any type of information that had to be protected. Many technologies had been developed to the long one of the time to guarantee that this happened of the best form, but the control has currently only not demonstrated to be enough efficient, when it is about an extensive organizational environment. This paper approaches the methodologies that can be applied to guarantee the management of security information, based in best practices, giving emphasis in to ITIL methodology, and show to an implementation of this methodology in the corporative environment and the gotten results and the benefits reached with the methodology.

Keywords: security information, methodology, IT, management, ITIL.

ITIL NA GESTÃO DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação, desde seu princípio visou assegurar o controle e o acesso dos sistemas/usuários a todo e qualquer tipo de informação que devesse ser protegida. Diversas tecnologias foram desenvolvidas ao longo do tempo para garantir que isso acontecesse da melhor forma, mas atualmente somente o controle não tem demonstrado ser suficientemente eficiente, quando se trata de um ambiente organizacional extenso. Este artigo aborda as metodologias que podem ser aplicadas para garantir a gestão da segurança da informação, baseadas nas melhores práticas, dando ênfase à metodologia ITIL, e mostra uma implementação dessa metodologia no ambiente corporativo e os resultados obtidos e os benefícios alcançados com a metodologia.

Palavras-chave: segurança da informação, metodologia, gestão, TI, ITIL.

I – Introdução

Muito se tem comentado e falado a respeito de segurança da informação, sendo esta atualmente, uma das áreas com maior foco em toda a cadeia de valor da Tecnologia da Informação.

É fato que a segurança da informação evoluiu para proporcionar um ambiente mais seguro e transparente tanto para os usuários, quanto para os administradores de redes de computadores, mas estes mesmos administradores têm, em sua grande maioria, uma visão específica e técnica com relação a esse tema.

Cada vez mais torna-se necessário uma visão de gestão da segurança da informação, para, dentre outros pontos, planejar, prever e atuar nos impactos causados pelo comprometimento da segurança de uma informação.

Através de metodologias das quais pode-se destacar o ITIL (*Information Technology Infrastructure Library*), são especificados os relacionamentos que a área da segurança da informação tem com as demais áreas da empresa, como por exemplo, os impactos financeiros causados por uma quebra de sigilo.

Além das metodologias que podem ser empregadas, também faz-se necessária a adequação às normais e leis vigentes em cada país, mas acima de tudo as empresas vêm demonstrando um padrão *de facto*, quando se trata de normas internacionais, sendo a Lei Sarbanes-Oxley a mais utilizada atualmente pelas empresas e órgãos governamentais.

O objetivo deste artigo é mostrar a segurança da informação, além dos aspectos técnicos, relacionados principalmente ao controle do acesso à informação, mas sim, ter uma abordagem sob a perspectiva de gestão e das melhores práticas, com ênfase na Metodologia ITIL, apresentando os conceitos e resultados obtidos com a implementação destas premissas de gestão da segurança da informação.

Na seção 2 são mostrados os principais conceitos e características envolvendo a segurança da informação. A seção 3 apresenta a metodologia ITIL, com ênfase nos aspectos relacionados à segurança da informação. Na seção 4 são mostrados os resultados efetivos da implementação da metotologia ITIL no ambiente corporativo e na seção 5 são feitas as considerações finais.

II – Conceitos e características da segurança da informação

A informação, principalmente em sua forma eletrônica, deve estar cada vez mais acessível e disponível a todo lugar e a qualquer momento. Quando se trata de Internet, os conceitos de tempo/localidade praticamente caem por terra, uma vez que a mesma informação pode ser acessada simultaneamente tanto por uma pessoa situada no prédio do servidor dessa informação, como por outra pessoa do outro lado do mundo, onde fatores como distância, e até mesmo o fuso-horário (horário em que a informação foi acessada) devem ser levados em consideração.

Diversas formas de ataque para obtenção de acesso à informação privilegiada podem ser estruturadas, como por exemplo, a invasão por *software* que é uma forma de acesso não autorizado a um equipamento, com aquisição da elevação de privilégios e execução de ações além daquelas previamente autorizadas, podendo tomar a forma de um vírus ou um *trojan*[1].

Independente de quaisquer aspectos, algumas premissas devem ser respeitadas, e quando se trata de segurança da informação, de uma maneira geral, alguns aspectos devem ser abordados, como por exemplo (STALINGS, 2006):

- **Confidencialidade**: Este aspecto refere-se especificamente à autenticação e ao acesso da informação, ou seja, quais usuários e/ou dispositivos devem ter acesso total ou restrito a determinado tipo de informação, devendo ser autênticos com relação à esse acesso.
- **Integridade**: Aspecto referente à alteração da informação, pois mesmo quando é obtido o acesso à informação a autenticidade ainda deve ser preservada, portanto deve-se ter claramente o controle de leitura, alteração e exclusão da informação.
- **Disponibilidade**: Além de disponível somente para sistemas/usuários devidamente autorizados, a informação, principalmente quando se trata de informação crítica, deve ser passível totalmente em ser recuperada, e vários procedimentos devem ser implementados para se conseguir a recuperação

[1] *Trojan* ou cavalo de tróia são programas de computador que podem capturar os nomes e senhas dos usuários do sistema.

da informação, quer seja através de rotinas de *backup*, quer seja através de redundância da informação, como por exemplo a tecnologia *raid*[2].

Para garantir o acesso e controle dos dados trafegados em uma rede de computadores, diversas ferramentas e tecnologias podem e devem ser empregadas, das quais são mais amplamentes usadas:

1. ***Firewall´s***: conceito de segurança que têm como princípio fundamental o controle no acesso à informação, podendo ser implementado totalmente baseado em *hardware* específico, ou em *software*, com a utilização de sistemas operacionais de apoio. O princípio básico de funcionamento e configuração de um *firewall* refere-se à liberação/bloqueio de portas de comunicação das aplicações, onde regras específicas podem ser implementadas, de acordo com o perfil e necessidade do usuário/sistema. Um esquema básico de funcionamento de um *firewall* pode ser observado na Figura 1 (MENDES, 2005).

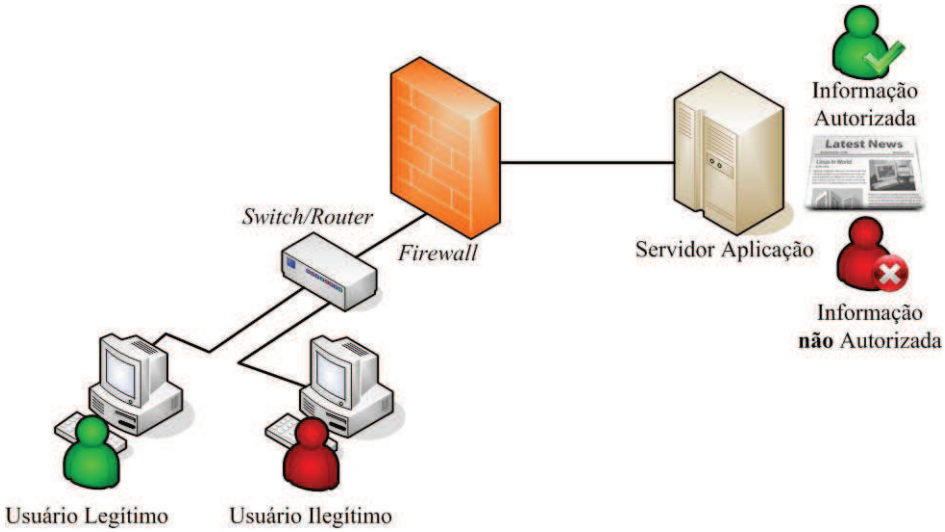


Figura 1: Esquema básico de funcionamento de *firewall*.

De acordo com a Figura 1, pode ser observado que a informação está disponível somente para o Usuário Legítimo, que possui as devidas permissões de acesso no *firewall*.

[2] Raid é uma tecnologia que refere-se a procedimentos que abrangem a replicação e/ou distribuição da informação em diversos meios de armazenamento.

Quando um Usuário Ilegítimo tentar acessar a informação, ela será negada devido às restrições do *firewall*.

2. ***IDS´s***: *Intrusion Detection System* ou Sistema de Detecção de Intrusos é um sistema que monitora o tráfego e detecta se a rede está tendo acessos não autorizados. Esta tecnologia visa detectar quando uma rede de computadores tem sua segurança comprometida, e, assim como os *firewall´*s pode ser totalmente baseada em *hardware* ou *software*.

3. ***IPS´s***: *Intrusion Prevention System*, ou Sistema de Prevenção de Intrusos, além de detectar o acesso irregular, também é capaz de tratá-lo, sendo na maioria dos casos, mais eficiente do que os próprios *IDS´s*.

Atualmente, as soluções para segurança de dados em redes de computadores reúnem-se em um único pacote que integra programas antivírus e *firewalls*. O chamado UTM – *Unified Threat Management*, ou Gerenciamento Unificado de Ameaças – surgiu para atender a demanda por soluções integradas e menos complexas, além de beneficiar o mercado com produtos mais baratos e mais eficientes.

Analistas e fornecedores declaram que o UTM deve evoluir para pacotes 3 em 1, que integram antivírus, *firewall* e soluções IDS/IPS. Para o mercado de segurança da informação, o UTM deve ser considerado um divisor de águas, já que as empresas que não seguirem o novo modelo provavelmente serão engolidas pelas empresas que integrarem seus produtos. O usuário, por outro lado, lucra com mais tecnologia, praticidade e baixo custo, podendo aumentar a quantidade e qualidade de suas ferramentas de segurança.

Embora eficientes, na maioria dos casos, somente soluções técnicas não dão uma visão estratégica e tática da segurança da informação, então faz-se necessário a adoção de metodologias que visam suprir essa necessidade técnica.

III – Metodologia ITIL

ITIL (*Information Technology Infaestructre Library)* são as diretrizes das melhores práticas desenvolvida pela CCTA (*Central Computer and Telecomunications Agency*), atu-

al OGC (*Office Government Commerce*) da Inglaterra, para o governo britânico no final dos anos 80 (ITSMF, 2006).

Atualmente, a metodologia ITIL é um padrão *de facto* na área de gerenciamento de serviço. Ela contém documentação especializada, pública e acessível, para o planejamento, provisão e suporte dos serviços de TI, além de fornecer as bases para a melhoria do uso, da eficiência e da eficácia da infraestrutura de TI, onde as organizações com interesse em serviços de TI, empregados de centros de computação, fornecedores, especialistas e consultores fazem parte do desenvolvimento desta metodologia.

A metodologia ITIL descreve uma abordagem sistemática e integrada para gerenciar os serviços de TI. A biblioteca enfatiza a importância de satisfazer os requisitos da empresa de modo econômico e orienta a área de TI para a prestação de serviço, focada no cliente, embora não descarte que em muitas empresas seja necessária uma mudança cultural para atingir esse benefício.

Adicionalmente, com a ajuda dessa metodologia, será criado um conjunto de terminologia no setor de serviço que padronizará a comunicação entre as partes envolvidas. A adesão às melhores práticas preconizada pela metodologia ITIL, trazem os seguintes benefícios diretos para a organização:

- Suporte aos processos de negócios às atividades desenvolvidas pelos responsáveis pelas decisões relacionadas a TI.
- Definição de funções, regras e responsabilidades no setor de serviços.
- Redução de despesas dos processos de desenvolvimento, procedimentos e instruções de trabalho.
- Os serviços de TI passam a atender os requisitos de um negócio específico.

E como benefícios indiretos, podem ser citados:

- Melhoria da satisfação do cliente através de maior qualidade, mensurável, na disponibilidade e na performace dos serviços de TI contratados.
- Melhoria da produtividade e eficiência através do uso planejado do conhecimento e experiência armazenados.
- Estabelecer as bases para uma abordagem sistemática do gerenciamento da qualidade no gerenciamento dos serviços de TI.

- Melhoria na satisfação da equipe de TI e consequente aumento da retenção dos empregados da empresa.
- Melhoria na comunicação e troca de informações entre o pessoal de TI e dos clientes.
- Treinamento e certificação dos profissionais de TI.
- Troca de experiência profissional.

O ITSMF (*IT Service Management Forum*) é uma organização internacional, fundada em 1991, independente, dedicada ao gerenciamento do serviço de TI, que não possui fins lucrativos e é totalmente operada pelos seus membros.

Tem como objetivos principais o de desenvolver e promover as melhores práticas para o gerenciamento de serviço, ser um veículo para auxiliar os membros a melhorar a qualidade do serviço e estabelecer um fórum relevante para a troca de informações e experiências.

Um diagrama esquemático referente à aplicação da metodologia ITIL pode ser observado na Figura 2:

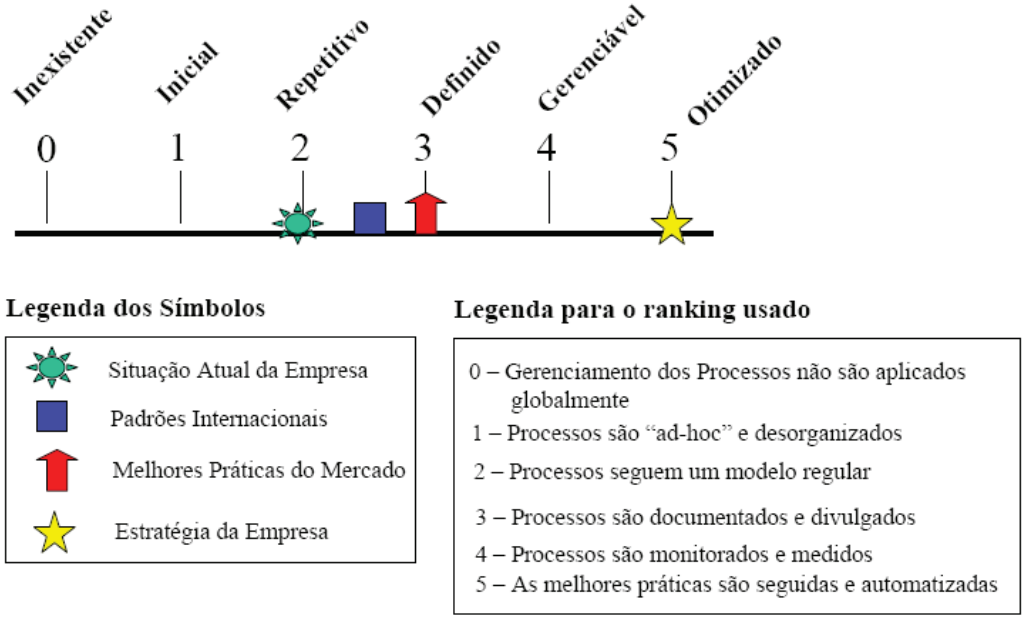


Figura 2: Diagrama de Implantação da Metodologia ITIL.

Toda a metodologia ITIL é baseada nos processos e em suas melhorias, sendo processo definido como um conjunto de atividades interrelacionadas e com um objetivo específico. Possui entradas de dados, informações e produtos para, através da identificação dos recursos necessários ao processo, transformar estas entradas nos objetivos específicos.

Processos são compostos de entradas, atividades e saídas, onde cada atividade pode conter funções executadas por pessoas ou automatizadas, e regras que definem como devem ser executadas as tarefas, conforme pode ser observado na Figura 3:

Figura 3: Definição de Processo.

A metodologia ITIL é baseada nas seguintes disciplinas e conceitos, que podem ser observados na Figura 4:

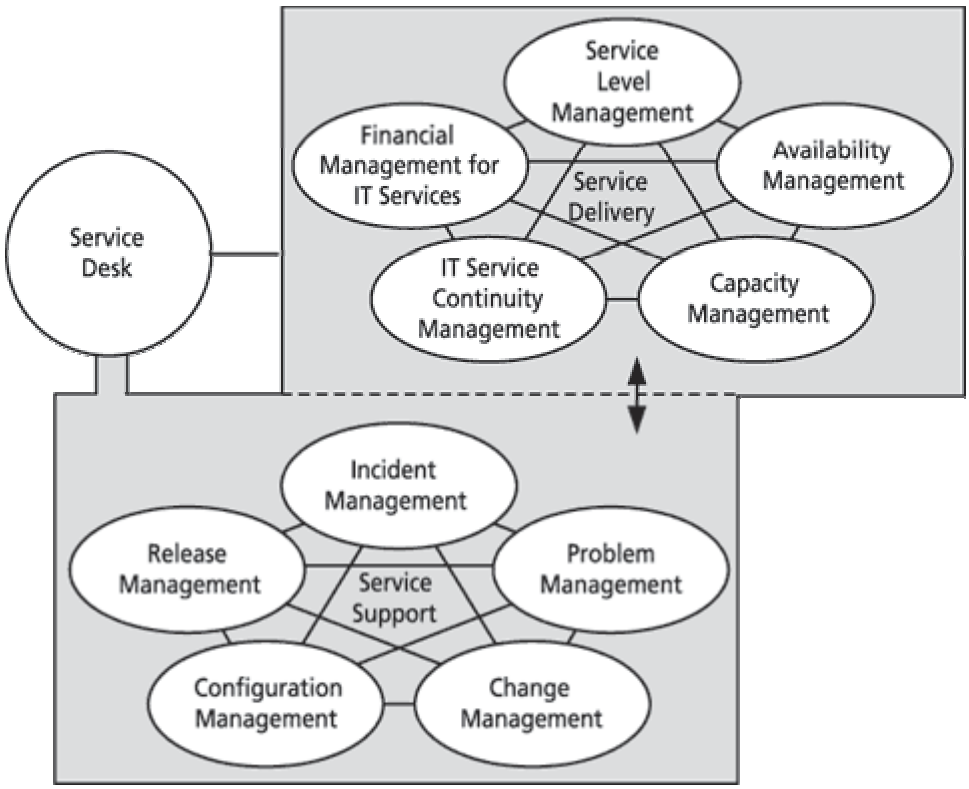


Figura 4: ITIL *Service Management*

- ***Configuration Management***: Gera informações para o *Financial Management for IT* para poder fazer a contabilização de gastos sobre os ativos de TI. Para o IT *Service Continuity Management* considerar os componentes no plano de continuidade de TI e para *o Availability Management* levantar riscos relacionados à disponibilidade.

- ***Change Management***: Tem relacionamento muito próximo com o processo de *Configuration Management* para levantar onde a mudança irá impactar. No *Release Management* para liberar as correções desenvolvidas.
- ***Release Management***: Tem dependência do processo de *Change Management* e utiliza o *Configuration Management* para registrar os *releases*.
- ***Incident Management***: Deve funcionar em conjunto com os processos de *Problem Management* e *Change Management*, mas o *Configuration Management* é importante para realizar análise de impacto, identificar soluções de contorno.
- ***Problem Management***: Necessita ter implementado já o processo de *Incident Management*.
- ***Service Level Management***: É importante já ter os processos de suporte implementados para suportar as SLAs.

Cada vez mais, a segurança torna-se um dos temas mais relevantes para gestores de TI. Um verdadeiro arsenal de regulamentações, metodologias e certicações, associado a um grande aparato de ferramentas de *hardware*, *software* e sistemas de prevenção está em permanente ebulição.

O Gerenciamento de Segurança é um processo que faz parte do *framework* do ITIL e que tem por finalidade controlar um nível definido de segurança para a informação e para os serviços e infra-estrutura de TI e capacitar os profissionais a compreenderem a importância do processo da segurança da informação na avaliação de riscos estruturais na TI, proporcionando aos participantes uma visão geral do Gerenciamento de Segurança do ITIL.

Gerenciamento da Segurança é uma das principais atividades em uma organização para manter as suas informações confidenciais e acessíveis apenas para quem deve ter real acesso, mesmo porque para os negócios atuais a informação na sua maioria é o centro de sua existência. Focado na implementação dos requisitos de segurança identificados no acordo de nível do serviço de TI (SLA – *Service Level Agreements*), a Gestão da Segurança tem dois objetivos principais:

- Satisfazer os requisitos de segurança dos SLA's, bem como outros requisitos, que dizem respeito a contratos, legislação e outras políticas impostas por fatores externos.

- Fornecer um nível básico de segurança, independente de outros requisitos externos.

A metodologia ITIL atua essencialmente na gestão de serviços de TI, cujos objetivos são:

- Alinhar os serviços de TI com as necessidades atuais e futuras das organizações e dos seus clientes e fornecedores.
- Melhorar a qualidade dos serviços de TI fornecidos.
- Reduzir, em longo prazo, o custo inerente à Disponibilização de Serviços de TI.

A Gestão da Segurança é uma atividade importante que tem como objetivo, por um lado controlar a disponibilização de informação e por outro evitar a utilização não autorizada dessa informação. Mais uma vez aqui a Internet (bem como as suas tecnologias associadas como sejam as Intranets e as Extranets), e o negócio eletrônico com os novos modelos de relacionamentos de empresas em rede (ligando clientes e fornecedores), têm um papel decisivo na medida em que as organizaçõoes de certa maneira se "abriram" para o exterior, aumentando drasticamente os riscos de intrusão colocando novos desafios para os seus responsáveis.

Por outro lado, também deve-se ter atenção que a infra-estrutura dos sistemas e tecnologias de informação e comunicação é muito mais complexa, o que implica que as organizações estão mais vulneráveis a problemas técnicos, erros humanos e ações intencionais que se traduzem na prática, por exemplo, por ataques de *hackers* e de vírus de computador. Esta crescente complexidade vai requerer uma abordagem integrada que é, na metodologia ITIL, dada pelo processo da Gestão da Segurança.

Os SLA's são um dos componentes mais importantes do processo de Gestão da Segurança na metodologia ITIL (embora a sua aplicação não se limite apenas nessa metodologia). Um SLA é um acordo formal, contrato escrito, onde constam os níveis de serviço (por exemplo, garantir que um *site* da Internet está disponível 24 horas por dia, 365 dias por ano ou que a reparação de um sistema que deixou de funcionar demorará menos de ***x*** horas), incluindo a segurança da informação, que o prestador de serviços de TI se compromete a cumprir.

Além dos SLA's deve-se ainda considerar os *OLA´*s – *Operational Level Agreements* (níveis de serviço operacionais) que fornecem uma descrição detalhada de como os serviços de segurança da informação devem ser prestados.

A metodologia ITIL define ainda outros documentos sobre a segurança da informação (ITEC , 2008):

- **Políticas de segurança da informação**: recomenda que as políticas de segurança devam partir dos responsáveis da organização e devem conter:
    1. Objetivos de segurança de informação para a organização.
    2. Metas e princípios de gestão sobre a forma como a segurança da informação deve ser gerida.
    3. Definição das funções, e responsabilidades, para a segurança da informação.
- **Planos de segurança da informação**: descrevem como é que as políticas devem ser implementadas para um determinado sistema de informação e/ou unidade de negócio.
- **Manuais de segurança da informação**: documentos operacionais para utilização diária com instruções operacionais detalhadas sobre a segurança de informação.

Entre suas várias disciplinas, a metodologia ITIL define um modelo de gerenciamento de segurança da informação. No entanto, diferentemente das normas tradicionais voltadas para a gestão desse quesito, como a ISO 17799 e BS7799, o código de boas práticas dessa metodologia dá uma visão de segurança sob a perspectiva da gerência de TI, sendo essa disciplina integrada nas outras do modelo.

Um dos fatores de maior atração para um gestor de segurança, ao estudar a metodologia ITIL, é a percepção de que as outras disciplinas do conjunto devem adotar técnicas de segurança dentro de seus processos, o que leva cada líder, seja o de *Change Management* ou de *Configuration and Asset Management*, a ser diretamente responsável por segurança dentro de sua própria área.

Apesar disso, sob o ponto de vista da metodologia ITIL, os controles pertinentes são centralizados nos processos de gerenciamento de segurança da informação. Essa perspectiva muda a forma como o tema deve ser visto dentro de uma corporação. Com essa metodologia, cada unidade tem a responsabilidade de desenvolver seus processos pensando

em segurança. Não se altera, no entanto, a responsabilidade do gestor de segurança desenhar as políticas da empresa a partir de um modelo reconhecido. A própria BS7799 é apontada como o modelo ideal (e segundo sua perspectiva, o padrão definitivo de normas voltadas para o assunto) que deve ser considerado por cada empresa no momento de escrever suas políticas.

Por se tratar de uma metodologia voltada a serviços de TI, baseadas nas melhores práticas do mercado, a metodologia ITIL vem sendo amplamente pelas empresas com esse foco e negócio.

IV - Implementação da Metotologia ITIL no ambiente corporativo

Como exemplo de aplicação e resultados práticos, será apresentada a implementação, o acompanhamento e a evolução da implantação da Metodologia ITIL no ambiente corporativo.

A empresa que serviu como base de pesquisa para este trabalho é a CTBC Telecom, como sede na cidade de Uberlândia, no estado de Minas Gerais. A CTBC Telecom é uma operadora de telecomunicações, e possui, dentre seu *portfólio* de produtos e serviços, o serviço de *Data Center*, que será o estudo específico deste trabalho.

O histórico desta implantação, vem desde o início do ano 2000, quando a empresa efetivamente consolidou e abriu o negócio de *Data Center*, tendo como primeiros clientes, a hospedagem de servidores de um *shopping center*, de um órgão de imprensa local e de um cliente corporativo.

No ano de 2001 foi sendo ampliado o escopo do negócio de *Data Center*, com equipe de suporte, monitoramento e *backup* própria, onde além dos clientes terem um serviço de melhor qualidade e valor agregado, também passaram e ter uma maior segurança com relação aos quesitos de disponibilidade dos sistemas e servidores hospedados no *Data Center*.

Ao longo dos anos, houve uma ampliação da infraestrutura do *Data Center*, com a migração da própria estrutura da CTBC Telecom para este *Data Center*, o que pode comprovar e consolidar a eficiência e segurança dos serviços prestados e embora o escopo do ambiente fosse aumentado com o decorrer do tempo, alguns pontos não tiveram a devida atenção.

Fez-se então necessário uma análise *SWOT*[3], que é um sistema analítico que representa Forças-Fraquezas-Oportunidades-Ameaças, e serve para identificar os pontos fracos de um concorrente, se tornando uma ferramenta útil para examinar oportunidades estratégicas. As **Forças** são definidas como sendo as vantagens competitivas da empresa. **Fraquezas** são as desvantagens. **Oportunidades** são as características dentro de um representativo mercado que podem oferecer a empresa vantagens competitivas. **Ameaças** são condições neste mesmo mercado que possam ser uma ameaça ou um bloqueio as oportunidades para esta empresa.

A análise SWOT da CTBC Telecom realizada para os produtos e serviços do *Data Center*, realizada em julho de 2006, pode ser obervada na Tabela 1:

Tabela 1: Análise *SWOT* - CTBC Telecom

Forças	Fraquezas
• Tecnologia Moderna. • Talentos Humanos Especializados. • Respeito da Marca CTBC Telecom.	• Ausência de Processos de Gestão de Tecnologia da Informação. • Dependência Excessiva de Pessoas.

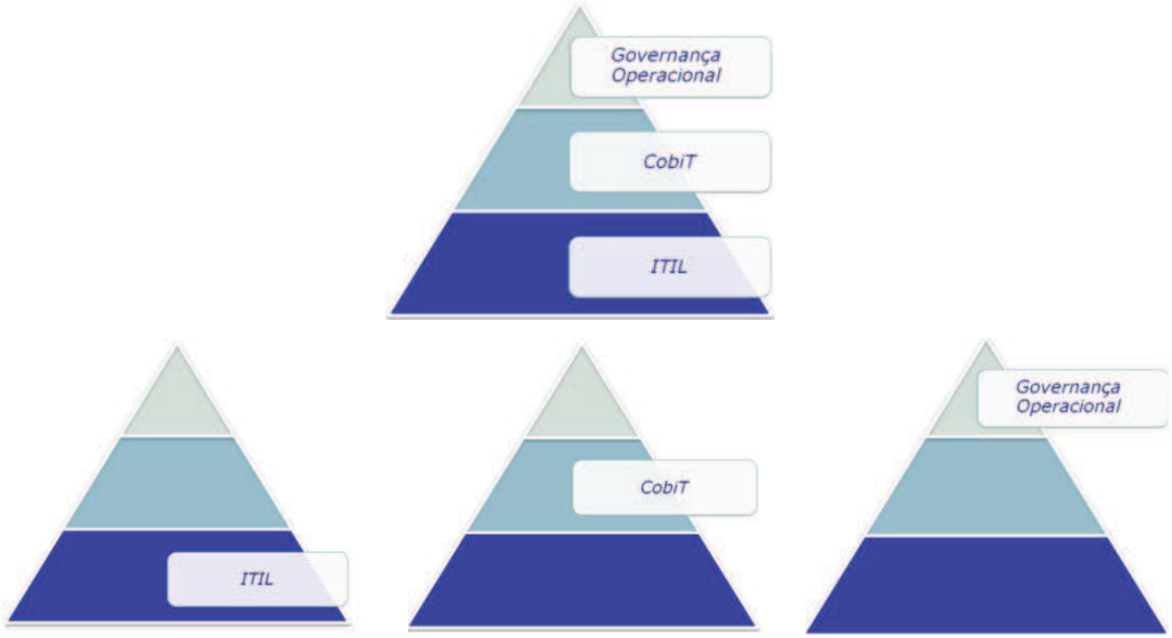
Oportunidades	Ameaças
• Implantar Processos de Gestão de Tecnologia da Informação. • Otimizar a Utilização da Tecnologia da Informação. • Aumentar a Geração de Receita em Clientes Atuais.	• Penalidades Contratuais pelo não Atingimento dos Níveis de Serviço Contratados. • Perda de Cliente por Alto Volume de Indisponibilidades. • Presença de Concorrentes Altamente Competitivos.

Como pode ser observado, mesmo possuindo toda a infraestrutura e recursos técnicos para a operação de um *Data Center*, os principais possíveis pontos de falha, referiam-se aos processos e pessoas envolvidas, além de uma clara falta de metodologia de trabalho. Diante deste cenário, algumas ações poderiam ter sido tomadas:

[3] Forças (*Strengths*), Fraquezas (*Weaknesses*), Oportunidades (*Opportunities*) e Ameaças (*Threats*).

- **Soluções paliativas**: continuar tentando resolver os problemas em decorrência da falta de padronização e metodologia de trabalho ou simplesmente aumentar o número efetivo de pessoas, que impactaria diretamente no custo da operação.
- **Soluções efetivas**: implementar efetivamente metodologias de trabalho, baseadas nas melhores práticas do mercado, como o ITIL e o Cobit.

As duas metodologias não são concorrentes, mas sim complementares, uma vez que cada uma delas tem seu papel bem definido, e são a base de apoio para uma efetiva governança operacional, como pode ser observado na Figura 5:



- Gestão dos serviços.
- Disponibilidade dos ambientes.
- Otimização de recursos.
- Melhorar relacionamento com cliente.

- Os objetivos esperados foram atingidos.
- Entregar o que foi ofertado da melhor maneira possível, considerando maior qualidade, reduzindo os custos, gerenciando os riscos e maior alinhamento da TI ao negócio CTBC Telecom.
- Identificar como está em relação ao mercado e as melhores práticas.
- Melhorar continuamente os processos.

- Maximizar os objetivos e estratégias de negócio da organização.
- Adicionar valores aos serviços entregues.
- Balancear os riscos.
- Obter retorno sobre os investimentos.

Figura 5: Estrutura de Gestão

O COBIT (*Control Objectives IT and Related Technology*) foi desenvolvido pela ISACA (*Information Systems Audit and Control Association*), é mantido pela instituição de Governança de TI, sendo uma prática internacional para a implementação de: (COBIT, 2008)

- Processos de TI.
- Direcionamento de TI, Monitoramento de TI e *Benchmarking*.
- Sistemas de Controles Internos.
- Governança de TI.

Como principais pontos fortes, o COBIT permite que TI aborde riscos não endereçados explicitamente por outros modelos e que seja aprovada em auditoria e funciona bem com outros modelos de qualidade, principalmente a metodologia ITIL, embora possua as limitações de dizer o que fazer, mas não como fazer, não trata diretamente desenvolvimento de *software* ou serviços de TI e não fornece um *roadmap* de aprimoramento contínuo dos processos.

Diante dessa situação, optou-se em executar um planejamento estratégico e com foco principal na implementação da metodologia ITIL na empresa, visando especificamente os serviços de *Data Center*, que é o objeto de estudo deste trabalho. O planejamento teve as seguintes diretrizes:

- Definir a missão e a extensão do processo.
- Iniciar uma campanha de comprometimento.
- Descrever as etapas do processo e procedimentos.
- Determinar responsabilidade, atividades e autoridade e para todos os envolvidos (regras).
- Determinar as necessidades de treinamento.
- Se necessário, selecionar e implantar ferramentas.
- Definir os tipos de relatórios (gerenciais, informativos e controle).
- Fazer melhoramentos contínuos nos processos.
- Implementar os processos.

Um resumo desse planejamento pode ser observado na Figura 6:

Figura 6: Melhores práticas de implementação.

A partir daí pode-se determinar claramente o escopo desse projeto:

- **Missão**: Garantir disponibilidade e continuidade das soluções de tecnologia, atuando pro-ativamente na identificação, gestão e atendimento de oportunidades.
- **Objetivos**:
  - **Perspectiva Financeira**:
    - Reduzir os Custos de Operação.
    - Cumprir Planejamento de Custos e Investimentos.
    - Identificar Oportunidades para Aumento na Geração de Receita.
  - **Perspectiva de Clientes:**
    - Gerenciar o Ciclo de Vida dos Serviços de Tecnologia da Informação.
    - Aprimorar o Relacionamento com os Clientes.
  - **Perspectiva de Processos Internos:**
    - Implantar processos de gestão de TI reconhecidos (ITIL).
    - Definir e utilizar documentos e ferramentas padronizados.
    - Gerenciar o Ciclo de Vida dos Processos.
  - **Perspectiva do Aprendizado e Crescimento:**
    - Certificação da equipe nas melhores práticas de TI (ITIL).
    - Domínio da inteligência do negócio de Data Center.

O *RoadMap* do projeto pode ser observado na Figura 7:

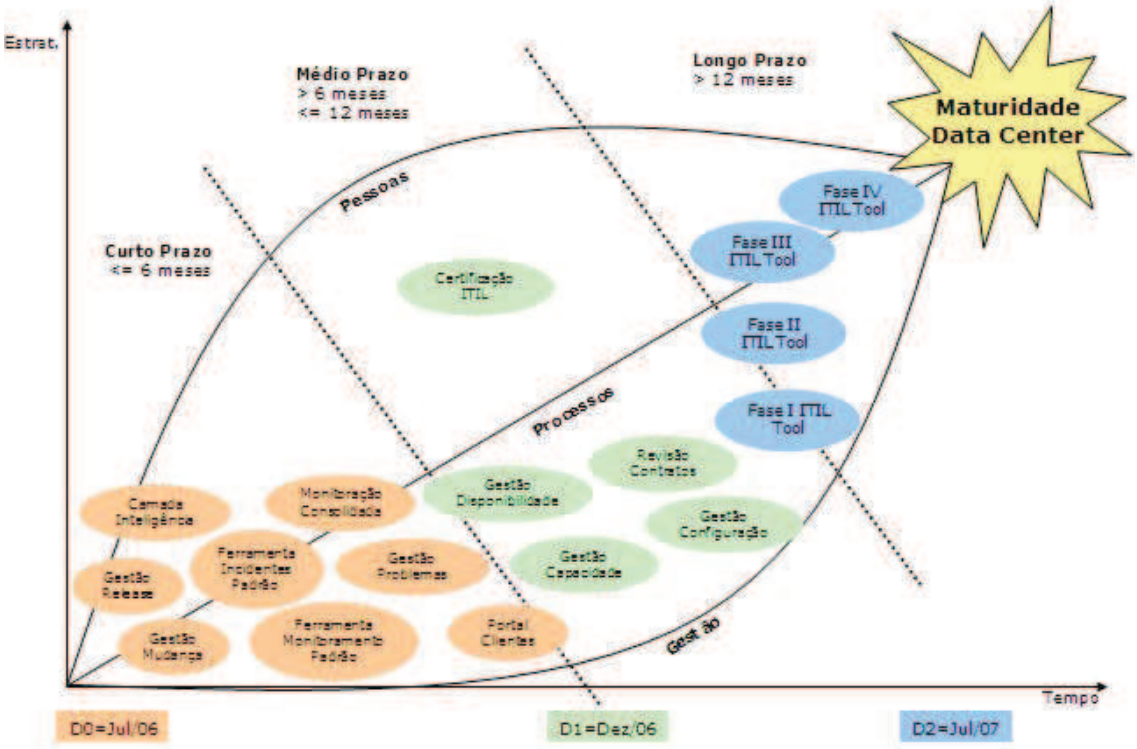


Figura 7: *RoadMap* – Agosto 2006.

- **Resultados esperados**:
  - **Curto Prazo**:
    - Base única e centralizada de casos.
    - Controle e gerenciamento dos incidentes.
    - Redução de trabalho operacional e erros.
    - Domínio da inteligência envolvida na prestação do serviço.
    - Redução nas indisponibilidades no ambiente.
    - Controle das mudanças no ambiente tratando os riscos.
    - Monitoramento de TI de um ponto único (sinergia):
      - Padronização da ferramenta de monitoramento.
      - Gerenciamento de todos os ativos de TI.
    - Geração de alarmes e notificações.
    - Melhoria no relacionamento e a satisfação dos clientes.
    - Disponibilização de informações do ambiente aos clientes.
    - Identificação da causa raiz dos problemas no ambiente.

- **Médio Prazo (6 meses)**:
  - Alocação adequada dos custos dos contratos.
  - Controle e gerenciamento de configuração do ambiente.
  - Identificação e aproveitamento da capacidade ociosa no ambiente.
  - Garantia da disponibilidade do ambiente através da identificação de oportunidades de melhoria.
- **Longo Prazo (12 meses)**:
  - Profissionalização do negócio *Data Center*.
  - Reconhecimento do mercado em melhores práticas.
  - Automatização dos processos da metodologia ITIL.

- **Riscos esperados:**
  - Atrasos na solução de problemas emergenciais.
  - Problemas decorrentes de erros de utilização.
  - Falta do *CMDB*:[4]
    - Ler configurações nos equipamentos.
    - Ativações de um cliente podem impactar os demais.
  - Falta de *Configuration*:
    - Gasto de tempo desnecessário para tratar incidentes.
  - Gestão de capacidade reativa:
    - Demora na resposta de necessidades efetivas.

Com a adoção da metodologia ITIL na CTBC Telecom, começou-se a ter um efetivo modelo de trabalho, com funções e atividades bem definidas, que culminaram numa melhoria na qualidade dos processos, bem como um aumento na qualidade dos serviços prestados aos clientes, principalmente através da implantação do processo de mudança (*changes*) e através do acompanhamento realizado e foram obtidos os resultados que podem ser observados respectivamente nas Figuras 8 e 9:

[4] *CMDB* (*Configuration Management Data Base*) é um banco de dados que contém todos os detalhes relevantes de cada item de configuração e detalhes dos relacionamentos importantes entre os itens de configuração.

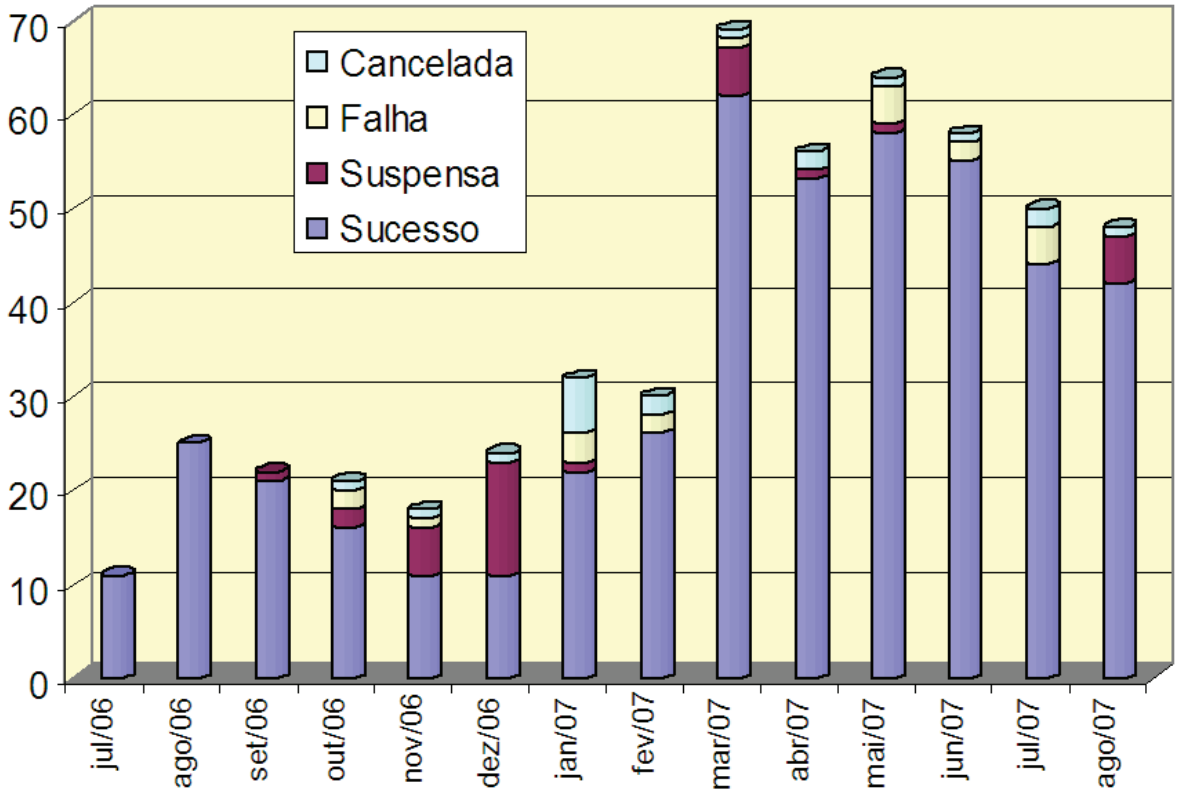


Figura 8: Resultados das *Changes.*

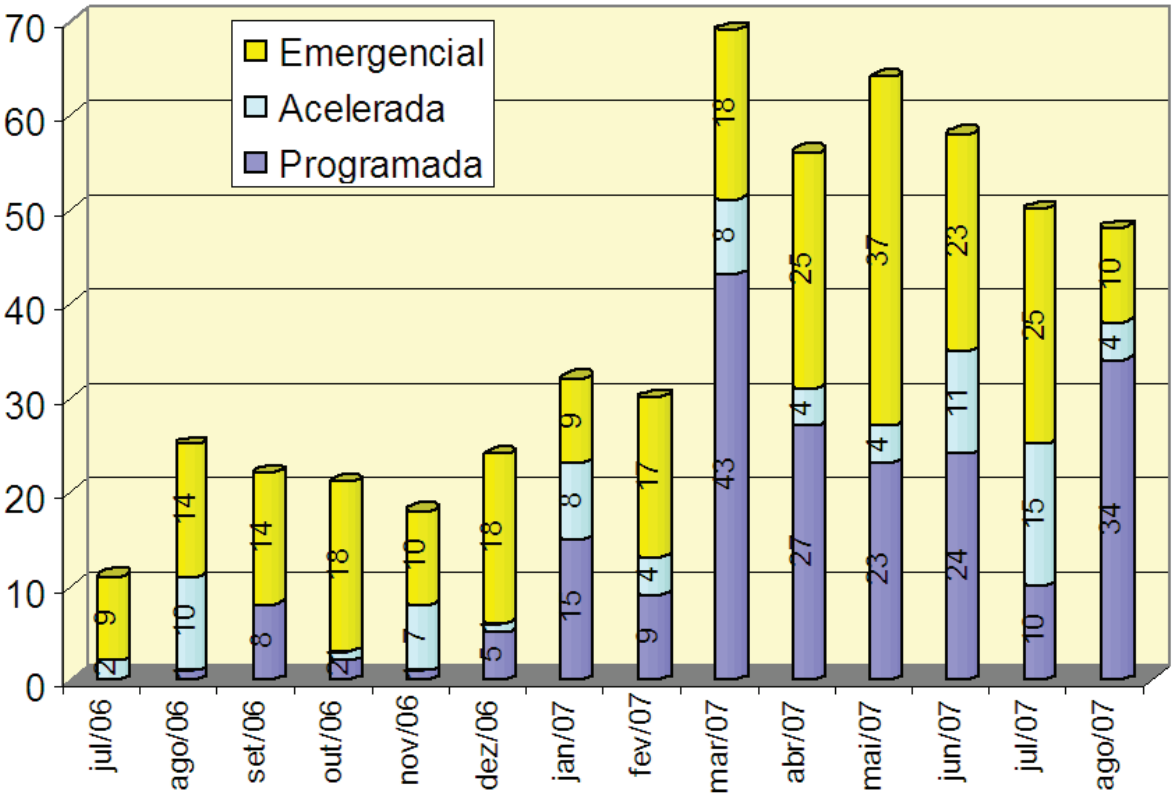


Figura 9: Resultados por Tipo de *Changes.*

Como resultados efetivos observaram-se:

- Redução das indisponibilidades dos serviços.
- Maior confiabilidade dos profissionais na infra-estrutura.
- Aproximação entre clientes e profissionais.
- Redução do tempo de atendimento de incidentes.
- Aumento da previsibilidade do ambiente de 14% para 46%.
- Melhoria de 79% para 89% do sucesso de mudanças.
- Redução das corretivas para menos de 24%

E podem ser comprovados através das Figuras 10 e 11:

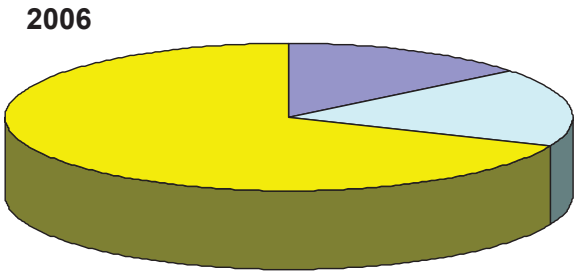


Figura 10: Resultados comparativos por Tipo de *Changes* – 2006.

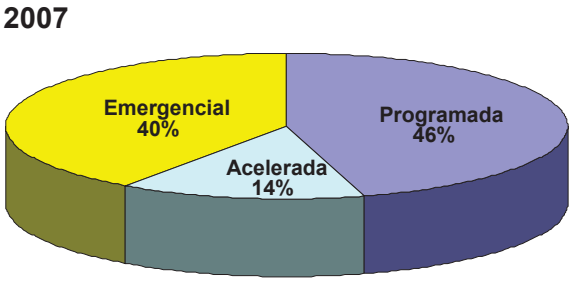


Figura 11: Resultados comparativos por Tipo de *Changes* – 2007.

V – Considerações Finais

Os benefícios em se utilizar a metodologia ITIL como referência para serviços de TI já são amplamente reconhecidos no mercado e a utilização de modelos baseados em melhores práticas está se tornando cada vez mais consolidada. Modelos desta natureza tradu-

zem práticas experimentadas, testadas e reconhecidas, tendo, assim a credibilidade de suas informações como pontos fortes.

O aspecto da segurança definido na politica de segurança, podendo envolver serviços e mecanismos de *hardware* e *software* para serviços de controle de acesso, integridade de dados e comunicação, confidencialidade, não-rejeição, disponibilidade de recursos e autenticação e as medidas de segurança de informação estão aumentando rapidamente em termos de aplicação, complexidade e importância.

Especificamente no caso da CTBC Telecom, esse reconhecimento se concretiza na forma de novos negócios, novos clientes, e principalmente em novas formas de prestação de serviços, tendo essa empresa sido reconhecida por mídia nacional como sendo um dos 10 melhores *Data Centers* do Brasil, conforme reportagem da revista especializada Info Exame, em sua edição de Maio de 2007.

Conforme pode ser observado, a efetiva implementação de uma metodologia pode trazer resultados que podem ser comprovados, traduzindo tanto em benefícios diretos, como a redução do custo operacional, como em benefícios indiretos, como o aumento da satisfação da qualidade dos serviços prestados aos clientes da empresa, e dentro da linha de melhores práticas do mercado, a metodologia ITIL vem mostrando sua eficiência e eficácia dentro das organizações.

Referências Bibliográficas

COBIT. ISACA – Serving IT Governance Professionals. Disponível em <http://www.isaca.org>. Acesso em: 20 jan 08.

ITEC. A ITIL e a governan»ca de TI – Itec. Journal. Disponível em: <http://www.itec.com.br/journal/40/itil.htm>. Acesso em: 20 jan 08.

ITSMF. *Foundation of IT Service Management, based on ITIL*. 2.ed. ITSMF-NL, 2006.

MENDES, Rogério. Segurança de dados em redes sem fio de computadores. In: 2º CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO, 2005, São Paulo. *Anais...* São Paulo: CONTECSI, 2005.

STALLINGS, W. *Cryptography and Network Security: Principles and Practice*. 4. ed. Englewood Cliffs, NJ: Prentice Hall, 2006.