

UNIVERSIDADE PRESBITERIANA MACKENZIE

FELIPE SANTOS FERREIRA

IMPACTOS E INFLUÊNCIAS DO GERENCIAMENTO DE REDES

São Paulo
2008

FELIPE SANTOS FERREIRA

IMPACTOS E INFLUÊNCIAS DO GERENCIAMENTO DE REDES

Trabalho de Conclusão de Curso apresentado ao Curso de Engenharia de Telecomunicações, da Universidade Presbiteriana Mackenzie, como requisito parcial à obtenção do grau de Especialista em Engenharia de Telecomunicações.

ORIENTADOR: Prof. Ms. Antônio Newton Licciardi Júnior

São Paulo
2008

AGRADECIMENTOS

Agradeço a Deus o grande criador de tudo, pela oportunidade de estar estudando, e principalmente pelo desejo de estar contribuindo em prol de todos.

Agradeço a meus pais, pois sem todo o esforço empreendido por estes, eu não teria educação e formação para desenvolver este projeto.

Agradeço a minha esposa pela compreensão e paciência durante a fase final da monografia.

Ao professor Newton, pela sua dedicação e competência.

RESUMO

Apresenta os impactos e as influências do gerenciamento de redes, bem como descrever as possibilidades de alcançar ou não uma maior disponibilidade e confiabilidade do sistema com a implantação de boas práticas de Mercado, que se descrevem como sendo ferramentas disponíveis no mercado, além de comparar seus respectivos desempenhos em estudo de casos. Aborda o conceito do protocolo SNMP e o conjunto de suas especificações de gerenciamento, onde inclui o protocolo, as definições de estruturas e dados e outros conceitos associados. Identifica a importâncias de implantar o gerenciamento de redes e planejar o gerenciamento de todos os processos envolvidos para obter o sucesso no gerenciamento da rede. Verifica que o gerenciamento de serviços é um conjunto formado por pessoas, ferramentas e processos que colaboram para assegurar a qualidade dos serviços e a satisfação dos clientes. Conclui apresentando os impactos desastrosos que pode ocorrer no caso de não por em prática o gerenciamento de rede e as influências boas que podem ser proporcionadas ao negócio com a prática do gerenciamento de rede.

Palavras-chave: Gerenciamento. Disponibilidade. Confiabilidade. Serviços. Satisfação.

ABSTRACT

Presents the impacts and influences the management systems, and describe the possibilities of achieving or not the increased availability and reliability of the system with the implementation of best practices research, which describe themselves as marketing tools available and to compare their performance in studies. Discusses the concept of the SNMP protocol and set of specifications for management, which includes the protocol, the definitions and data structures and other associated concepts. Identifies the importance of deploying the network management and planning the management of all processes involved to achieve success in managing the network. Notes that the management of services is a group formed by people, tools and processes that help to ensure service quality and customer satisfaction. Concludes with the disastrous consequences that can occur if not implemented by the network management and the good influences which may be provided to deal with the practice of network management.

Keywords: Management. Availability. Reliability. Services. Satisfaction.

LISTA DE ILUSTRAÇÕES

Figura 1.	Estrutura de nomenclatura de Objetos do SNMP. (Mauro Schmidt, 2005).....	19
Figura 2.	Arquitetura SNMP. (RAD, 2006).....	21
Figura 3.	Processo ITIL. (ITSMF, 2001)	25
Figura 4.	Serviço com Gerenciamento de Níveis de Serviço relacionado com cliente. (OGCb, 2001)	33
Figura 5.	Entradas e saídas do Gerenciamento de Disponibilidade. (OGCb,2001).....	36
Figura 6.	Processo de Gerenciamento de Disponibilidade.(OGCb,2001).....	38
Figura 7.	Exemplo de Gerenciamento Financeiro para serviço em TI. (Empresa Conecta, 2006).....	40

LISTA DE ABREVIATURAS E SIGLAS

IP	Internet Protocol
MIB	Management Information Base
ISO	International Organization for Standardization
OSI	Open Systems Interconnection
SNMP	Simple Network Management Protocol
IETF	Internet Engineering Task Force
TCP	Transmission Control Protocol
ARPANET	Advanced Research Projects Agency Network
FTP	File Transfer Protocol
RFC	Request for Comments
UDP	User Datagram Protocol
DDP	Apple Talk Datagram-Delivery Protocol
IPX	Novell Internet Packet Exchange
SMI	Structure of Management Information
ASN.1	Abstract Syntax Notation One
TI	Tecnologia da Informação
ITIL	Information Tecnology Infrastructure Library
NOC	Network Operation Center
SLA	Service Level Agreements
SLM	Service Level Management
OLA	Operational Level Agreements
UC	Underpinning Contract

SUMÁRIO

1	INTRODUÇÃO	09
2	GERENCIAMENTO DA REDE.....	10
3	IMPLANTAÇÃO DE REDUNDÂNCIA.....	15
4	ESPECIFICAÇÃO DE GERÊNCIA POR REDUNDÂNCIA	16
5	PROTOCOLO SNMP	18
5.1	COMPONENTES.....	19
5.1.1	MIB – MANAGEMENT INFORMATION BASE	19
5.1.2	SMI – STRUCTURE OF MANAGEMENT INFORMATION.....	20
5.1.3	SNMP V1	20
5.1.4	SNMP V2	21
5.1.5	SNMP E SEUS AGENTES E GERENTES	21
6	VANTAGENS E DESVANTAGENS DO SNMP	22
7	GERENCIAMENTO DE PROCESSOS	24
8	CENTRAL DE SERVIÇOS.....	27
9	SUPORTE DE SERVIÇOS	28
9.1	GERENCIAMENTO DE INCIDENTES	28
9.2	GERENCIAMENTO DE PROBLEMAS	29
9.3	GERENCIAMENTO DE MUDANÇAS.....	30
9.4	GERENCIAMENTO DA CONFIGURAÇÃO	31
9.5	MÉTRICAS DO GERENCIAMENTO.....	32
10	ENTREGA DE SERVIÇOS	33
10.1	GERENCIAMENTO DO NÍVEL DE SERVIÇO.....	33
10.2	GERENCIAMENTO DE DISPONIBILIDADE.....	36
10.3	GERENCIAMENTO DA CAPACIDADE	37
10.4	GERENCIAMENTO DA CONTINUIDADE DOS SERVIÇOS	38
10.5	GERENCIAMENTO FINANCEIRO	40
10.6	AUDITORIA DO PROCESSO DE GERENCIAMENTO	41
11	ESTUDO DE CASOS.....	42
12	CONCLUSÃO.....	43
	REFERÊNCIAS	45

1 INTRODUÇÃO

Com o crescimento dos sistemas de telecomunicações, aliado ao aumento do tráfego das redes de dados, e como consequência do avanço tecnológico, a estrutura das redes de telecomunicações foi se tornando cada vez mais sofisticadas, tendo a necessidade do surgimento de uma gerência de redes (SOARES NETO, 1990).

O gerenciamento de uma rede consiste em se saber, em tempo real, o desempenho da rede por meio de uma monitoração, estabelecendo um controle sobre o desempenho da mesma.

Soares Neto (1990) conceitua a gerência de redes como sendo a realização de uma coleta de dados, obtidos em intervalos de tempos regulares, seguido de um tratamento específico em cada segmento da rede, comparando-os a um modelo de desempenho pré-estabelecidos.

Leinwand e Conroy (1999) consideram fundamental a utilização de uma ferramenta de monitoração em tempo real das informações dos equipamentos da rede, sendo indispensável à utilização de gráficos.

Laudon e Laudon (2002) fornecem técnicas para elaboração dos critérios no momento da escolha do melhor sistema de gerenciamento de rede, um sistema que não apenas gerencie, mas também possibilite a configuração dos elementos.

Este trabalho tem o intuito de apresentar os impactos e as influências do gerenciamento de redes, bem como descrever as possibilidades de alcançar ou não uma maior disponibilidade e confiabilidade do sistema, com a implantação de boas práticas de Mercado, que se descrevem como sendo ferramentas disponíveis no mercado, além de comparar seus respectivos desempenhos em estudo de casos.

Este trabalho será organizado em quatro partes, sendo que a primeira descreverá o funcionamento de um gerenciamento de redes, seus conceitos e suas aplicações.

Em seguida, se procederá a uma descrição das influências do gerenciamento de rede em empresas de diversos setores e a importância dada ao gerenciamento de rede em cada uma destas empresas.

Na terceira parte serão abordados os impactos do gerenciamento de rede nessas empresas, analisando seus pontos fortes e fracos.

Por fim, serão realizados estudos de casos analisando tanto a influência quanto os impactos gerados na implantação do gerenciamento de rede, efetuando análise estatística das vantagens e desvantagens da implantação das boas práticas no gerenciamento de redes.

2 GERENCIAMENTO DE REDE

Segundo Leinwand e Conroy (1990) organizações investem muito dinheiro na construção de um complexo centro de gerenciamento. Contratam especialistas de rede para se dedicarem ao monitoramento e verificação do desempenho do sistema, com o objetivo de evitar uma possível parada do mesmo.

O gerenciamento das redes destas empresas deve levar em consideração o controle de seus processos, buscando maximizar a eficiência e a produtividade do sistema.

Leinwand e Conroy (1999) consideram o gerenciamento de uma rede como sendo o processo de monitorar múltiplos sistemas a partir de um componente específico da rede. Um software que gerencia a plataforma da rede ou de diferentes redes possui as seguintes funcionalidades nele incluídas: gráfico de utilização da rede, mapeamento da rede, base de dados da rede e eventos de desempenho e erros da rede.

Para conseguir realizar o gerenciamento de uma rede, é fundamental que nesta rede os membros estejam conectados uns aos outros ou de alguma forma todos os membros devem comunicar-se com algum outro dispositivo da rede. Estes membros da rede devem entender claramente o que uns comunicam com os outros ou ao dispositivo o qual esta ocorrendo à comunicação, para que a comunicação efetiva possa ocorrer.

Segundo Gallo e Hancock (2003) um conceito básico importante de ser lembrado é que praticamente todos os dispositivos de redes usam algum método para que sejam identificados de forma única.

Esta forma única pode ser um endereço IP (*Internet Protocol*), um protocolo ou pode ser um dispositivo que não tem nenhuma identificação, contudo reportam os problemas por meio da console no próprio dispositivo.

De acordo com Leinwand e Conroy (1999) o gerenciamento de falhas é o processo de localização e correção de problemas ou falhas na rede. Consiste em identificar a ocorrência de falhas na rede, isolando a causa de falha e corrigindo a mesma se possível.

Os benefícios de gerenciar o processo de falha é que quando ocorre um determinado problema, a detecção e a recuperação do mesmo é mais rápida, diminuindo o tempo de indisponibilidade da rede.

Podemos seguir três processos no gerenciamento de falhas: identificação da falha, isolar a causa da falha e se possível a correção da falha.

Na identificação do problema a verificação do número de falhas e das causas é muito importante e essencial, na medida em que se torna necessário priorizar as mais

importantes para inicializar a correção das falhas. Depois se devem isolar as causas do problema, que podem influenciar na falta de conexão do restante da rede, e finalmente deve-se buscar a correção da falha, pois a mesma pode gerar prejuízo, devido à indisponibilidade da rede.

Gerencia de falhas é uma das funções chaves do sistema de gerência de redes integradas, tem a finalidade de localizar, determinar as causas e, se possível, corrigir falhas na rede. Os sistemas de gerência de falhas devem ser capazes de funcionar corretamente na presença de falhas na rede.

Grande parte dos sistemas de monitoração apenas permite examinar os objetos de gerência de agentes livres de falhas.

Leinwand e Conroy (1996) afirmam que os objetos de gerência refletem o estado das entidades gerenciadas. Assim, a leitura da MIB (*Management Information Base*) de um agente falho muitas vezes é útil para se determinar a razão porque um determinado elemento da rede está falho ou inacessível. A MIB foi conceituada na seção 5.1.1.

Gerência de rede é fundamental para controlar e monitorar as operações de rede conforme os requisitos dos usuários, inclui a inicialização, monitoração e modificações tanto nos elementos de hardware quanto de software.

A classificação proposta pela ISO (*International Organization for Standardization*) em cinco áreas, referente às funcionalidades do gerenciamento de redes: falhas, desempenho, configuração, segurança e contabilização. Foram propostas como parte da especificação do gerenciamento de sistemas OSI (*Open Systems Interconnection*).

Entendendo melhor o modelo OSI: o propósito deste modelo de referência que é uma norma internacional, é proporcionar uma base comum à coordenação do desenvolvimento de normas para a interligação de sistemas, enquanto assegura igualmente a continuidade através da consideração dos sistemas atuais, enquadrando-os no modelo de referência.

O termo interligação de sistemas abertos (OSI) pretende qualificar normas para a troca de informação entre sistemas abertos entre si para o propósito de comunicar, utilizando mutuamente as normas especificadas.

O fato de um sistema ser aberto não implica uma implementação particular do sistema, tecnologia ou meios de interligação, mas refere ao reconhecimento mutuo de sistemas e suporte das normas aplicáveis.

É igualmente objetivo desta norma a identificação das áreas para desenvolvimento ou melhoria de normas, e modo de proporcionar uma referência comum para

manter a consistência entre normas semelhantes. Não é objetivo de a norma servir de especificação para implementação ou constituir a base para avaliação da compatibilidade das implementações atuais. Igualmente, não pretende fornecer um detalhe tão fino que determine precisamente os serviços e protocolos da arquitetura de interligação. Em disso, o modelo oferece uma referência conceitual e funcional que permite a equipes internacionais o desenvolvimento produtivo e independente de normas para cada nível do modelo OSI.

Modelo de referência de sistemas abertos (à cooperação com outros sistemas).

Objetivos:

- criar uma base comum que permita a coordenação do desenvolvimento de normas;
- criar uma referencia comum para manter consistência entre normas relacionadas;
- permitir a identificação de áreas de desenvolvimento e melhoramento de normas;

Uma grande preocupação do modelo OSI é, sendo relativamente geral ser também flexível, a razões genéricas que levaram à adoção deste modo foram:

- normalmente divisões correspondem a demarcações de caráter físico ou lógico (cabos ou controlo de erros, encaminhamentos)
- fazer divisões quando há mudanças de endereços
- fazer divisões quando há multiplexação
- tentar agrupar funções que utilizem elementos comuns
- o modelo OSI tem em atenção à existência de serviços de interface já disponíveis
- tentar encontrar um número razoável de camadas, nem muito grande nem muito pequeno.

O SNMP (*Simple Network Management Protocol*) é o padrão de fato utilizado atualmente no gerenciamento das redes, é um framework aberto desenvolvido pela comunidade TCP/IP que permite o gerenciamento integrado de redes altamente heterogêneas.

O protocolo de controle de transmissão/protocolo Internet o TCP/IP (*Transmission Control Protocol – Internet Protocol*) Protocolo de Controle de Transmissão –

Protocolo de Internet, é um conjunto de protocolos de padrão industrial criado para conexões de redes de larga escala abrangendo ambientes de rede local e de rede de longa distância.

Como mostra a representação cronológica a seguir, as origens do TCP/IP datam de 1969, quando o Departamento de Defesa dos Estados Unidos nomeou a *Advanced Research Projects Agency Network* (ARPANET).

A ARPANET foi resultado de um experimento de compartilhamento de recursos. O objetivo era fornecer links de comunicação para redes de alta velocidade entre vários supercomputadores localizados em várias regiões dos Estados Unidos.

Os primeiros protocolos, como Telnet (para emulação de terminal virtual) e o protocolo de transferência de arquivo FTP (*File Transfer Protocol*), foram desenvolvidos primeiramente para especificar utilitários básicos necessários para o compartilhamento de informações pela ARPANET. Com o crescimento da ARPANET, tanto em termos de dimensão quanto de escopo, surgiram dois outros protocolos importantes:

Em 1974, o protocolo de controle de transmissão (TCP) foi apresentado como uma especificação provisória que descrevia como criar um serviço de transferência de dados confiável de host a host em uma rede.

Em 1981, o protocolo Internet (IP) foi apresentado de forma provisória e descrevia como implementar um padrão de endereçamento e pacotes de rotas entre redes interconectadas.

No dia 1 de janeiro de 1983, a ARPANET começou a exigir o uso padrão dos protocolos TCP e IP para todo o tráfego e comunicação essencial de rede. A partir dessa data, a ARPANET começou a ficar mais conhecida como a Internet e os protocolos necessários começaram a ficar mais conhecidos como o conjunto de protocolos TCP/IP.

O conjunto de protocolos TCP/IP é implementado em inúmeros produtos de *software* TCP/IP disponíveis para uso em várias plataformas de computação. Atualmente, o *software* TCP/IP continua amplamente usado na Internet e é muitas vezes utilizado para a criação de grandes conjuntos de redes privadas e roteadas.

Harrington, Presuhn e Wijnen (2002) conceituam que originalmente a arquitetura SNMP é baseada no paradigma gerente-agente, na qual a rede é monitorada e controlada através de aplicações de gerenciamento chamadas gerentes executando numa Estação de Gerência de Rede (*Network Management Station*), e agentes executando nos nós e dispositivos da rede.

Cada agente executando numa rede mantém informações de gerência armazenadas numa base de informações de gerência local denominada MIB (*Management*

Information Base). A Estação de Gerência da Rede executa uma coleção de aplicações de gerência que permite o gerenciamento de falhas, desempenho, configuração, segurança, contabilização, entre outras funcionalidades.

Empregado pelas aplicações gerentes e agentes para comunicar informações de gerência, o protocolo SNMP é usado pelos gerentes para consultar e controlar os agentes, e pelos agentes para disparar *traps* e respostas às consultas executadas pelos gerentes. O protocolo SNMP oferece uma coleção de operações a fim de comunicar as informações de gerência.

A IETF (*Internet Engineering Task Force*) definiu três arquiteturas de gerenciamento para a internet durante os anos 90, conhecidas como SNMPv1, SNMPv2, e SNMPv3.

3 IMPLANTAÇÃO DE REDUNDÂNCIA

Um problema inerente aos sistemas é a potencial vulnerabilidade a falhas. Contudo, é possível introduzir redundâncias, e assim, tornar um sistema como um todo mais confiável do que as suas partes.

Segundo Leinwand e Conroy (1996), em um sistema de computação é impossível tolerar todos os tipos de falhas. Assim, o objetivo da tolerância a falhas é melhorar a confiabilidade de disponibilidade de um sistema ao tolerar um número específico de tipos de falhas. Modelos de falhas têm sido desenvolvidos para descrever de maneira abstrata os efeitos dos tipos de falhas.

O modelo de falha mais amplo é o modelo de falha Bizantino, neste modelo os componentes falham de maneira arbitrária. Este modelo acomoda todas as possíveis causas de falhas, incluindo falhas maliciosas.

Este tipo de falha ocorre, por exemplo, um processo bizantino pode tentar assumir a identidade do outro, enviar mensagens com valores incorretos, duplicar mensagens ou simplesmente não enviar mensagens que o protocolo especificar.

A redundância é normalmente introduzida pela replicação dos componentes ou serviços, embora replicação seja um conceito intuitivo, sua implantação em sistemas requer técnicas sofisticadas.

Técnicas de replicação tais como *coordinator-cohort*, que é uma variante da replicação passiva, a replicação semi-passiva, e semi-ativa são variantes das duas principais classes. A técnica de replicação passiva é também conhecida como abordagem *primary-backup*, onde é selecionada uma réplica servidora para atuar como réplica primária, e as outras réplicas atuam como *backup*. Desta forma, a comunicação entre uma aplicação cliente e as réplicas servidoras ocorre somente através da réplica primária.

Uma aplicação confiável deve assegurar que os serviços sejam oferecidos mesmo em presença de falhas. Nós consideramos que devido os atuais sistemas de gerência de redes e a abstração de grupos cooperantes de processos é possível aplicar uma variação da técnica de replicação passiva para construir sistemas de gerência de redes tolerantes a falhas.

Um grupo de agentes poderia ser estendido para enviar suas informações, isto é, seus objetos de gerências para outros agentes de forma a replicar suas informações e tais agentes atuem como réplicas *backups* dos seus objetos de gerência.

4 ESPECIFICAÇÃO DE GERÊNCIA POR REDUNDÂNCIA

Segundo Guerraoui e Schiper (1997), existem inúmeras possibilidades de implantar redundância em sistemas com o objetivo de obter Confiabilidade. Os recursos de comunicação e processamento disponíveis numa rede são requisitos que devem ser considerados na definição da estratégia de redundância a ser utilizada.

A disponibilidade de tais recursos torna-se mais importante em situações de falhas, onde normalmente o comportamento da rede é afetado e a quantidade de recursos de comunicação e processamento é reduzida.

Com o objetivo de aplicar o mínimo de recursos da rede, alguns requisitos operacionais devem ser identificados na arquitetura para replicação de objetos de gerência, e ao mesmo tempo garantir a distribuição dos objetos replicados em lugares específicos da rede.

São: Flexibilidade, Disponibilidade, Consistência e Escalabilidade.

- Flexibilidade: a arquitetura permite a definição dos objetos de gerência replicados por um *cluster*. O *Cluster* que pode ser definido como um sistema onde dois ou mais equipamentos trabalham de maneira conjunta para realizar processamento pesado. Em outras palavras, os equipamentos dividem as tarefas de processamento e trabalham como se fossem um único computador

- Disponibilidade: as cópias dos objetos replicados são mantidas em lugares específicos, assim quando houver uma cópia dos objetos que seja acessível, sem falhas, o acesso às informações desses objetos é garantido.

- Consistência: os valores dos objetos de gerência replicados em diferentes lugares da rede têm que estar consistentes com a cópia original.

- Escalabilidade: com o aumento do número dos agentes monitorados, requer a utilização de mais recursos da rede na replicação dos objetos de gerência. Para diminuir os recursos utilizados, a arquitetura permite a redefinição ou a criação de novos agrupamentos, assegurando a escalabilidade da operação de objetos de gerência.

O modelo de agrupamento de agentes de gerência consiste de elementos de redes chamados nós, conectados numa rede.

Nos nós da rede ocorrem somente falhas do tipo *fail-stop*, isto é, um nó só funciona quando ocorrem falhas. Este modelo não considera falhas nos links de comunicação porque tais falhas podem implicar que nós operacionais sejam considerados falhos e, assim, as informações replicadas desses nós poderiam não refletir a realidade.

Assume-se que o nó gerente nunca falha e tem a capacidade de alguma forma de detectar um nó falho. O modelo também assume que certos nós com capacidade de processamento e espaço de memória podem ser expandidos para atuarem como gerente de *cluster*.

As informações de gerência são mantidas em variáveis chamadas objetos do *Cluster*. Os agentes somente mantêm informações locais sobre os nós onde estão hospedados, enquanto os gerentes informações locais e as replicadas de outros agentes. Cada *cluster* possui um gerente de *cluster*.

Os gerentes de *cluster* comunicam-se através de serviços de grupo, tais como *multicast* confiável e gerência de grupos, para suportar a consistência das informações replicadas.

O *Multicast* é a entrega de informação para múltiplos destinatários simultaneamente usando a estratégia mais eficiente onde as mensagens só passam por um link uma única vez e somente são duplicadas quando o link para os destinatários se divide em duas direções.

São definidas três operações de comunicação de forma que o gerente de *cluster* de um *cluster* possa desempenhar a tarefa de replicação dos objetos do *cluster* e também receber os objetos replicados de outros *clusters*: *query* (Consultar), *replicate* (Replicar), e *receive* (Receber).

Um gerente de *clusters* possui dois tipos de comunicação:

- Gerente de *cluster*-agente: é usada para monitorar os agentes membros de um *cluster*.

- Gerente do *cluster*-gerente de *cluster*: é usada para replicar os objetos nos agentes dos *clusters* pares.

5 PROTOCOLO SNMP

Segundo Stallings (1996), o SNMP não é apenas um protocolo e sim um conjunto de especificações de gerenciamento, onde inclui o protocolo propriamente dito, as definições de estruturas de dados e outros conceitos associados.

Seguindo as arquiteturas definidas pela IETF a versão SNMPv1 foi a descrição inicial do protocolo SNMP, através da RFC 1157, prevendo a sua operação sobre os protocolos UDP (*User Datagram Protocol*), IP (*Internet Protocol*), DDP (*AppleTalk Datagram-Delivery Protocol*) e IPX (*Novell Internet Packet Exchange*). Esta versão apresentou diversos problemas referente a segurança do gerenciamento.

RFC (*Request for Comments*) . Ele é um documento que descreve os padrões de cada protocolo da Internet previamente a serem considerados um Padrão.

O SNMPv2, descrito pelas RFC 1441 a 1450, ofereceu melhorias em segurança e funcionalidade, mas apresentou falhas nas áreas de autenticação, e na própria segurança.

Por fim, o SNMPv3, através da RFC 2271 a 2275, além de ser compatível com versões anteriores, inclui o controle de acesso ao protocolo, autenticação e a manutenção da privacidade da informação gerenciada.

5.1 COMPONENTES

5.1.1 MIB – MANAGEMENT INFORMATION BASE

A MIB é um conjunto de informações organizadas hierarquicamente provenientes da rede gerenciada organizadas. Essas informações são alocadas em um banco de dados de objetos gerenciados que podem ser acessados através de protocolos de gerenciamento de rede como o SNMP.

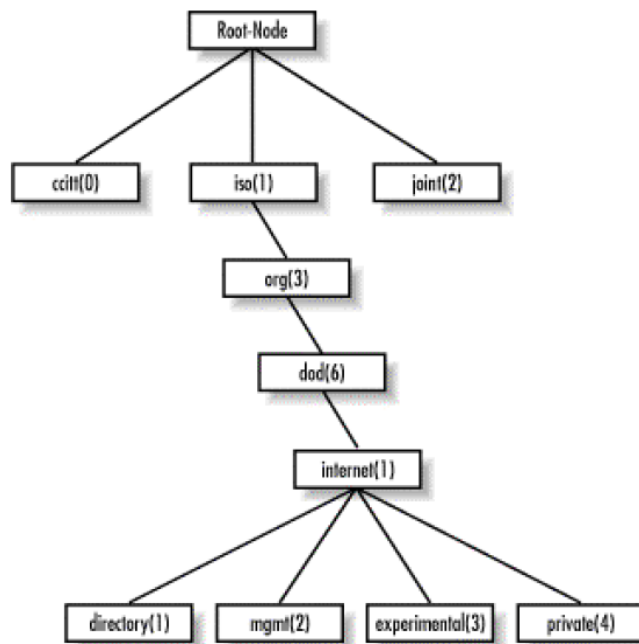


Figura 1. Estrutura de nomenclatura de Objetos do SNMP. Extraído de Mauro e Schmidt (2005).

Um objeto gerenciado que pode ser chamado de MIB, é uma das características de um elemento gerenciado. Um exemplo é apresentado na Figura 1.

Existem duas especificações para os objetos monitorados no gerenciamento de rede: o primeiro é denominado MIB-I que teve como objetivo incluir um número mínimo de objetos, e foi estabelecido um limite de 100 objetos. O segundo, e sucessor do MIB-I é denominado MIB_II, o número de objetos presentes é de 170. De acordo com Mauro e SCHMIDT, (2005) com as melhorias adquiridas a maioria dos fabricantes, a maioria implanta a MIB-II em seus equipamentos.

5.1.2 SMI – STRUCTURE OF MANAGEMENT INFORMATION

A SMI define regras para a descrição de informações de gerenciamento usando a notação ASN.1 (*Abstract Syntax Notation One*), que especifica a estrutura que nomeia com um único nome a cada objeto gerenciado na rede e os tipos de dados que são permitidos na MIB. A SMI faz três especificações chaves:

- tipos de dados ASN.1
- tipos de dados da SMI
- Tabelas MIB SNMP, descritos na seção a seguir 5.1.3

5.1.3 SNMPv1

A SMI do SNMPv1 especifica que todos os objetos gerenciados devem obrigatoriamente conter certo subconjunto de dados ASN.1. Dessa forma os três tipos de dados requeridos são:

- Nome
- Sintaxe
- Codificação

Os tipos de dados específicos da SMI são divididos em dados simples e dados de aplicação. Os dados simples incluem:

- Inteiros
- Octetos
- Strings
- Identificadores de Objetos

Os dados de aplicação são:

- endereço de rede
- Contadores
- Medidores
- Periodos de tempo
- Opaques
- Inteiros
- Inteiros sem sinal

5.1.4 SNMPv2

O SMI do SNMPv2 faz adições e melhorias aos tipos de dados específicos do SNMPv1.

- Cadeias de bits
- Endereços de rede
- Contadores
- Módulos MIB
- Declarações de compatibilidade
- Declarações de capacidade

5.1.5 SNMP E SEUS AGENTES E GERENTES

Os objetos gerenciados pelo SNMP são agrupados em um banco de dados virtual, chamado de base de informações gerenciais ou MIB. No que refere-se a arquitetura, uma rede gerenciada através do SNMP é composta por alguns elementos chaves, são estes:

- dispositivos Gerenciados
- agentes
- sistemas de gerenciamento da rede

O SNMP viabiliza a comunicação entre agentes para que os objetos correspondentes aos diversos dispositivos de rede possam ser acessados e modificados. Os dispositivos gerenciados são pontos de rede que contem agentes SNMP, como apresentado na Figura 2.

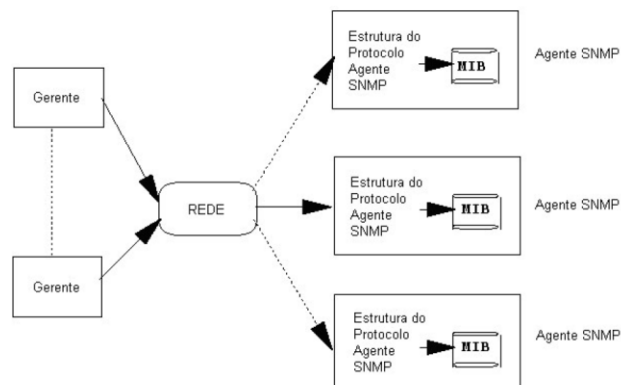


Figura 2. Arquitetura SNMP. Extraído de RAD (2006).

6 VANTAGENS E DESVANTAGENS DO SNMP

Uma rede compatível com SNMP oferece benefícios significativos. A possibilidade de administração, monitoração e controle eficaz de uma rede, de forma a se prevenir, detectar e corrigir falha, sem contar um desempenho satisfatório na rede em sua manutenção.

O SNMP requer pouca codificação para ser implantado, é extensível permitindo que fabricantes adicionem funcionalidades de gerenciamento a produtos já existentes. Também possibilita a ampliação da base de equipamentos que o suportam independente do fabricante, devido oferecer uma separação adequada de sua arquitetura. Permite que diferentes produtos de rede sejam gerenciados, pois é padronizado, provendo a rede à interoperabilidade desejada.

Outra vantagem é a eficiência na entrega dos pacotes do SNMP com a utilização do UDP como protocolo de transporte, resultante em menor processamento.

Vale lembrar algumas desvantagens na utilização do protocolo SNMP para o gerenciamento de redes.

Com o uso do protocolo de transporte UDP, o mais comum para o SNMP, aumenta-se a probabilidade de perdas de dados, pois este protocolo de transporte não faz a verificação de entrega e nem utiliza um mecanismo de verificação.

A primeira deficiência do protocolo SNMP é que tem algumas grandes falhas de segurança, que podem dar acesso a intrusos da rede à informações que transitam pela mesma. Intrusos também poderiam desligar alguns terminais. A solução para este problema é simples. Por causa da expansibilidade do SNMP, a mais recente versão de SNMP, SNMPv2, somou alguns mecanismos de segurança que ajudam a combater os três principais problemas de segurança: privacidade de dados (prevenir os intrusos de ganhar acesso a informação levadas pela rede), autenticação (impedir os intrusos de enviar falsos dados pela rede), e controle de acesso (que restringe acesso de variáveis particulares a certos usuários, removendo assim a possibilidade de um usuário derrubar a rede acidentalmente).

Na verdade, o SNMP provê pouco suporte para esquemas de autenticação. Ele suporta apenas um esquema de duas senhas. Uma senha pública permite ao administrador da rede pedir o valor de variáveis, e outra senha privada permite ao administrador da rede fixar valores de variáveis. Essas senhas são chamadas *communities*, e todo dispositivo conectado numa rede gerenciada por SNMP deve ter essas duas *communities* configuradas. Sempre ao menos uma das *communities* está presentes em cada mensagem do manager para o agente,

mas é descrita sem nenhuma proteção, como texto simples, propiciando falhas de segurança. Não é difícil um intruso descobrir as senhas e influir no funcionamento da rede.

Além da questão da segurança, SNMP é tão simples que a informação com a qual ele lida não é detalhada ou bem organizada o bastante para suportar redes muito grandes, além da carga de rede gerada pelo SNMP. Isto é principalmente devido à rápida criação do SNMP, pois ele nunca foi pretendido para conduzir administração de rede no ano 2000. Mesmo assim, é o protocolo mais utilizado atualmente.

Outros problemas podem ser citados: o protocolo não é muito eficiente, pois há a transmissão de muitos dados desnecessários; a organização das variáveis na árvore MIB também não é muito eficiente. Além, por usar endereçamento IP, se há um problema de roteamento na rede e um dispositivo não pode ser alcançado, é impossível monitorá-lo ou reconfigurá-lo.

7 GERENCIAMENTO DE PROCESSOS

Ineficiência no foco dos objetivos e mudanças efetuadas produz grande impacto no negócio, assim diminuindo a qualidade do serviço prestado.

O conceito de governança de TI existe nos negócios há um bom tempo, mas é bem recente a preocupação a este assunto, resultando de tendências atuais de negócios.

Muitas companhias ou departamentos de TI não adotam nenhuma metodologia para melhorar a qualidade do serviço prestado (interno e externo), criando insatisfação e perda de clientes. Este é um dos motivos que estas empresas façam investimentos em qualidade técnica e treinamento de profissionais para que estejam altamente qualificados nos serviços prestados, superando as expectativas e as necessidades dos clientes.

Para que o objetivo geral possa ser realizado, são necessários alguns objetivos específicos, assim vamos utilizar como base os processos ITIL (versão. 2):

- Descrever melhores práticas dos processos da metodologia ITIL;
- Descrever os processos de gerenciamento de mudanças;
- Identificar o escopo de atuação;
- Analisar os benefícios após a implantação do gerenciamento;
- Mudanças

O ITIL (*Information Technology Infrastructure Library*) é uma biblioteca de melhores práticas para o gerenciamento da infra-estrutura de TI, foi desenvolvida no final da década de 80 no Reino Unido pela agência governamental do país.

Inicialmente elaborado como um guia para o Governo Britânico, a biblioteca ao longo do tempo, provou ser útil para organizações em diversos setores através de sua adoção como base para o gerenciamento de serviços de TI.

As melhores práticas, na verdade, descrevem e documentam um conjunto de experiências definidas através de processos e que foram realizadas em várias organizações e que demonstraram resultados positivos, incentivando outras organizações a adotarem o ITIL.

A finalidade do planejamento é criar um plano do projeto que um gestor de projeto possa usar para acompanhar o progresso de sua equipe. O ITIL é considerado um padrão a nível mundial, reconhecido com sucesso por inúmeras empresas.

Segundo Magalhães e Pinheiro (2007), o gerenciamento de mudanças tem o objetivo de assegurar que os processos sofram modificações conforme o planejado e autorizado, garantindo a menor quantidade de impactos, garantindo a identificação dos itens

de configuração envolvidos, procedimentos de mudança testados e garantia de um plano de recuperação de serviço.

De acordo com Camurugy (2005), a ITIL traz algumas mudanças de paradigma, faz com que o negócio foque no valor e não no custo, faz pensar em toda a cadeia que envolve a prestação de serviços e transfere o olhar para processos e pessoas e não apenas na tecnologia.

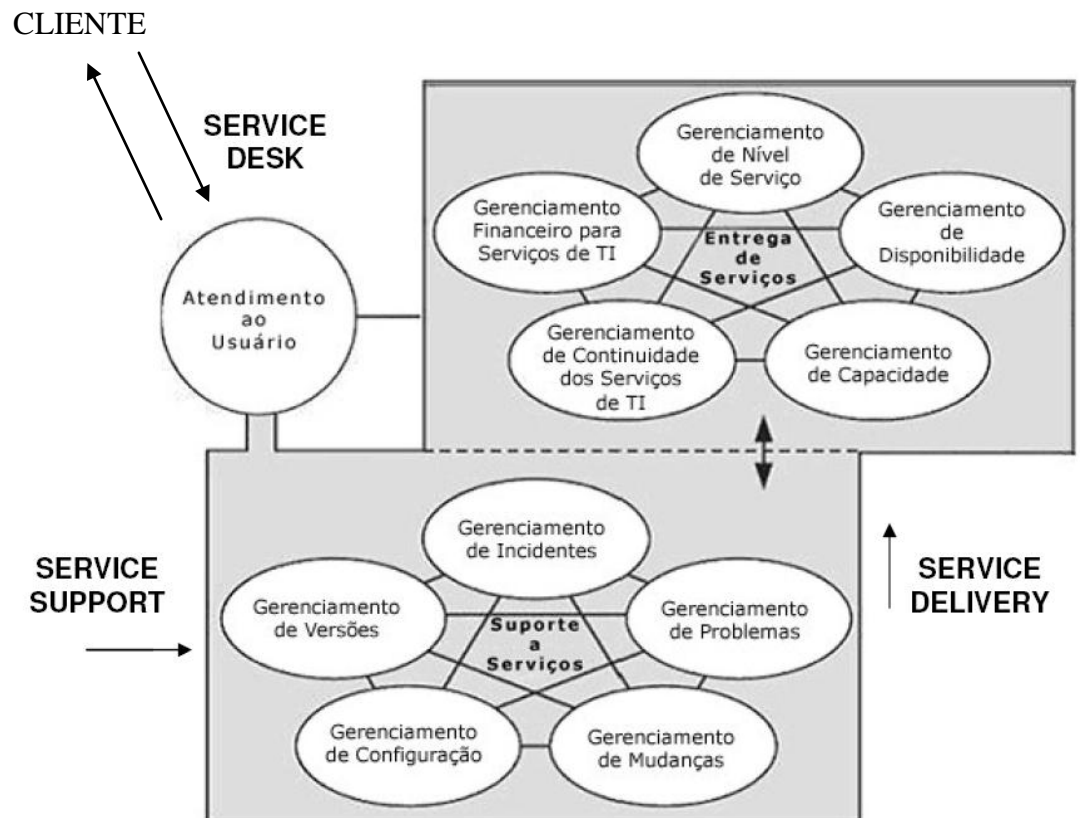


Figura 3. Processo ITIL. Extraído de ITSMF (2001).

A figura 3 ilustra os processos de gerenciamento de serviços separados de acordo com a necessidade de suporte ou entrega de serviços, tendo a Central de Serviços, o ponto único de entrada de chamados. Descritos nas seções do Capítulo 9.

O gerenciamento de serviço de TI é um conjunto formado por pessoas, ferramentas e processos que colaboram para assegurar a qualidade dos serviços, com suporte a níveis de serviços acordados previamente com os clientes.

O controle dos processos torna-se mais fácil quando ocorre o agrupamento das atividades, possibilitando o acompanhamento do desempenho.

A maioria dos benefícios de um programa de Gerenciamento de serviços pode levar um tempo para serem obtidos, contudo também existem benefícios em curto prazo. Os principais benefícios para a empresa de implantar uma metodologia para o gerenciamento de serviços são:

- melhor qualidade no serviço, com um suporte mais confiável;
- segurança e confiabilidade da continuidade dos serviços;
- visão mais clara da capacidade atual;
- fornecimento de informações gerenciais para acompanhamento de desempenho;
- equipe com maior motivação;
- gestão mais eficiente da infra-estrutura e dos serviços prestados;
- maior satisfação para os clientes;
- os processos são otimizados, consistentes e interligados;

8 CENTRAL DE SERVIÇOS

É importante separar dentro das operações de TI quem faz parte do suporte aos usuários e que vai realizar atividades de resolução de problemas e desenvolvimento.

A Central de Serviços é uma evolução do conceito de *Help Desk*. Este tradicionalmente atende problemas de *hardware* e auxilia a *softwares* básicos, e a Central de serviços atende todas as solicitações dos usuários relacionadas a qualquer serviço prestado pela área de TI.

Os objetivos da Central de Serviço são fornecer um único ponto de contato com o cliente, facilitar a restauração operacional do serviço com o mínimo de impacto para o negócio do cliente dentro dos níveis de serviços acordados com o cliente.

A infra-estrutura da Central de Serviços possui três camadas:

- Nível 1: Suporte por telefone e monitoração de sistemas, também monitora a infra-estrutura e equipamentos de TI.

- Nível 2: Suporte Local que é solicitado pelo Nível 1 para solução de incidentes no local de trabalho do cliente.

- Nível 3: Suporte especializado em solução de incidente. É composto por vários técnicos especializados nas áreas de servidores, telecomunicações, infra-estrutura, cabeamento, banco de dados, rede e controle de acesso.

A implantação de uma Central de Serviços pode trazer vários benefícios:

- aumento de Acessibilidade
- produtividade
- redução de Impacto
- disponibilidade no Atendimento
- percepção de qualidade e satisfação dos clientes
- indicadores para Gestão e suporte a decisão

9 SUPORTE DE SERVIÇOS

9.1 GERENCIAMENTO DE INCIDENTES

Um gerenciamento de Serviços de TI está orientado a entrega de níveis de serviços com qualidade e com a rapidez que o negócio exige, assim é necessário ter um processo de tratamento de incidentes eficiente e eficaz, capaz de monitorar os níveis de serviços.

Este é um dos processos mais importante, pois entrará em atuação a partir de incidente levantado por usuários ou ferramentas de monitoramento.

É vital para manter a agilidade dos serviços, considerarem que as informações dos incidentes levantadas neste processo serão de grande importância para o processo de Gerenciamento de Problemas.

Este processo de gerenciamento de incidentes tem como objetivo restaurar o serviço normal com a maior brevidade possível com o mínimo de interrupção, assim minimizando os impactos negativos nas áreas de negócio.

A maioria dos incidentes relativos ao processo de gestão de incidentes inicia-se de contatos, quando o NOC (*Network Operation Canter*) recebe um contato, é criado um novo incidente para registro e atualização de incidentes, o NOC também é responsável por executar com sucesso a gestão do incidente.

O resultado esperado do processo é a resolução definitiva do incidente, em alguns casos o incidente é causado por erros dentro da infra-estrutura de TI ou Telecom. Nesses casos, uma solução temporária é desenvolvida para restaurar o ambiente à produtividade.

9.2 GERENCIAMENTO DE PROBLEMAS

Os departamentos de TI têm como tarefa diária resolver problemas, muitas vezes inesperados. O grande volume de chamados com erros em sistemas, mau funcionamento dos componentes acaba gerando muito trabalho para a equipe de suporte.

O problema da qualidade da solução faz com que o incidente volte acontecer, assim ocupando o tempo novamente das equipes de suporte para a solução do incidente.

Uma forma de reduzir a quantidade de incidentes é evitando a sua recorrência. Com o processo de gerenciamento de incidentes estas falhas causadas não identificadas serão analisadas e corrigidas para que não voltem a ocorrer.

É preciso ter alguns cuidados no processo, registrar todos os erros conhecidos e soluções, pois com isto será possível fazer uma melhor gestão do conhecimento. Dependendo do ramo de negócio, algumas empresas conseguem fazer com que grande parte dos incidentes seja resolvida diretamente no primeiro nível, devido ao uso da base de conhecimento.

De acordo com a necessidade de negócio, prevenindo a recorrência de incidentes e registrando informações que melhore a maneira de tratamento dos problemas, resultam em níveis mais altos de disponibilidade e produtividade.

A ocorrência de alguns incidentes é inevitável, muitos outros incidentes são causados por erros de alguém da organização.

As principais causas do problema podem ser relacionadas a problemas operacionais, ao *hardware* ou *software*, a rede ou alguma mudança realizada sem prévia análise dos impactos que poderia causar.

O registro do problema é importante, pois permite a reconstituição do problema, o treinamento da equipe e análise de tendências de ocorrência de problemas. Esta classificação é fundamental para a metodologia de gerenciamento de problemas, pois permitem definir, de forma precisa, a velocidade e a eficiência que o problema será tratado. Com isso identificamos a causa do problema.

9.3 GERENCIAMENTO DE MUDANÇAS

Cada vez mais os usuários exigem níveis de serviços mais altos para alcançar os objetivos do negócio. A área de TI esta em constante mudança para atender a demanda da evolução do cenário de negócios, realizando implementações nos sistemas e mais capacidade para os serviços, criando novas políticas de segurança.

A maioria dos problemas relacionados com a qualidade dos serviços normalmente está relacionada a alguma mudança já realizada anteriormente. Estas mudanças, geralmente mal feitas, sem planejamento e testes adequados podem resultar em mais problemas, muitas vezes desastrosas, trazendo prejuízos ao negócio.

Diversos problemas de indisponibilidade dos serviços estão relacionados a uma falha de configuração do operador. É inaceitável falhas brutais nas mudanças implementadas, devido à dependência que temos dos serviços de TI.

9.4 GERENCIAMENTO DA CONFIGURAÇÃO

Segundo OGCa, (2001) com o armazenamento e gerenciamento de dados relacionados à infra-estrutura de TI, o processo de Gerenciamento da Configuração dá a organização de TI um controle maior sobre todos os ativos de TI.

O gerenciamento da Configuração tem como objetivo fornecer um modelo lógico da infra-estrutura de TI, identificando e controlando todos os ativos. É Considerado o processo central e que fornece suporte a outros processos da ITIL fornecendo informações sobre a infra-estrutura de TI.

A gestão de Configuração deve ter os seguintes objetivos:

- contabilizar todos os recursos de TI e configurações na empresa e seus serviços;
- fornecer informações precisas sobre configuração e documentação para suportar os processos de gerenciamento de serviços;
- analisar os registros de configuração e confrontar com a infra-estrutura, a fim de corrigir quaisquer exceções;

Controlar significa verificar e corrigir os registros de configuração, mostrando um nível maior de controle sobre a Infra-estrutura.

Os gestores de TI beneficiam de fato de terem estas informações precisas de configuração planejadas para os seus processos de gestão de serviços. A tomada de decisão torna-se mais fácil se possuir dados completos e precisos, o que resulta em melhores estimativas de desempenho e recursos.

Estes gestores poderão comprometer-se com níveis de serviço com maior confiança e a sua gestão de risco irão melhorar, reduzindo tempo de indisponibilidade não planejado no processo.

9.5 MÉTRICAS DO GERENCIAMENTO

Fazem parte da gerência da rede funções como supervisão e monitoração das sub-redes com seus equipamentos e recursos, medição da utilização dos recursos, configuração dos equipamentos para funcionamento, configuração dos canais de transmissão, disponibilidade de recursos, manutenção dos equipamentos, provisionamento, confidencialidade de dados, integridade de dados e controle de acesso.

A partir do estudo e análise de cada sistema desenvolvido foi possível identificar algumas necessidades básicas de definições, especificações e desenvolvimentos, a fim de se melhorar a qualidade do serviço oferecido, otimizar tarefas realizadas e integrar os sistemas.

Com a integração dos esforços da empresa visando gerência será alcançada através do aproveitamento dos recursos existentes, contemplando a planta atualmente instalada e sua respectiva infra-estrutura necessária à operação.

O preciso identificar as necessidades de especificação e desenvolvimento para a solução dos problemas atuais, adotando um modelo padronizado tanto para o desenvolvimento como para a integração, observando aspectos de distribuição de sistemas necessários para a gerência de uma rede complexa como a rede de telecomunicações e TI. Entre as ações que se deve realizar para solucionar os problemas relativos ao gerenciamento da rede pode-se enumerar os sistemas Gerenciados, determinar o escopo dos sistemas gerenciados, equipamentos de telecomunicações e TI ou conjunto destes equipamentos com funções específicas na planta.

Novos equipamentos, orientar a aquisição de novos equipamentos já objetivando gerência, através de uma arquitetura de gerenciamento. Plataformas de Gerenciamento, orientar a aquisição de uma plataforma de sistemas de gerência como suporte aos sistemas de gerência, definindo a rede de suporte para gerência, o *hardware*, o sistema operacional e o sistema gerenciador de banco de dados para a operação.

10 ENTREGA DE SERVIÇOS

10.1 GERENCIAMENTO DO NÍVEL DE SERVIÇO

Segundo FRY (2003), o processo de Gerenciamento de Níveis de Serviços gerencia o nível dos serviços prestados pela equipe de TI, ou seja, é o acordo feito entre o departamento de TI e os clientes, com o objetivo de definir o tempo de resolução par cada solicitação realizada pelos clientes e tempo para restabelecimento de cada indisponibilidade ocorrida na operação. Este acordo é chamado de Acordo de Nível de Serviço – *Service Level Agreements* (SLA).

Não podemos gerenciar expectativas, mas é possível gerenciar falhas. É importante que os acordos sejam formalizados para eliminar qualquer divergência ou discórdia entre as partes.

No caso de a empresa não possuir SLAs, não existirá nenhum acordo de nível de serviço, causando um constante conflito entre ambas as partes, empresa contratada e seus clientes.

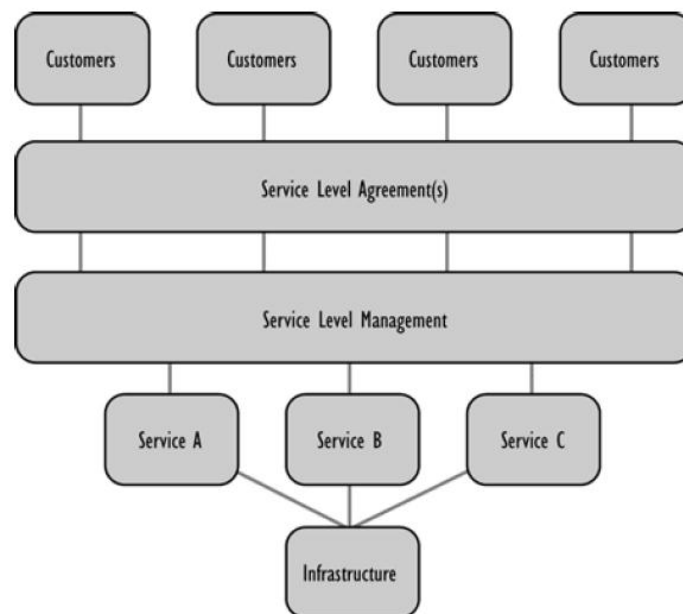


Figura 4. Serviço com Gerenciamento de Níveis de Serviço relacionado com Clientes. Extraído de OGCB (2001).

A Figura 4 exemplifica a relação entre cliente / serviço e o Gerenciamento de Nível de Serviço de determinada Empresa, ambos definem as características dos serviços e as responsabilidades de ambas as partes.

O SLM (*Service Level Management*) é o nome dado aos processos de planejamento, coordenação, acordo, monitoração e reporte de SLAs, além da revisão contínua da realização dos serviços, para assegurar que a qualidade requerida e a viabilidade financeira do serviço sejam mantidas e melhoradas.

Quando uma aplicação fica indisponível, ou um determinado equipamento danificado, as características do SLA é garantir para o cliente o tempo que o problema será solucionado, todavia a Central de Serviço terá um determinado tempo até a solução.

Um dos elementos mais conhecidos no Gerenciamento do Nível de Serviço são os SLAs, que permitem o departamento de TI e o cliente acordarem sobre quais serviços devem ser fornecidos, a disponibilidade necessária e seus custos.

Acompanhando o SLA, também temos no Gerenciamento de Nível de Serviço o Acordo de Nível Operacional - *Operational Level Agreement* (OLA) e Contratos de Apoio – *Underpinning Contract* (UC).

Segundo MAGALHÃES (2006) as diferenças entre SLA, OLA e UC são as seguintes:

O SLA é um acordo entre a área prestadora de serviços de TI e seus clientes, este acordo deve deixar claro quais serviços estão sendo oferecidos e o nível de cada serviço (hora de funcionamento, horário de suporte e outros).

Para prestar este serviço, o departamento de TI talvez precise contratar serviços de terceiros, assim tendo a necessidade de também ter um contrato formal que é dado o nome de UC.

Em alguns contratos para prover serviços para seus clientes, o departamento de TI precisa de serviços prestados por outras áreas da empresa, mas que não são terceiros.

O SLA é um acordo entre o provedor interno de serviços de TI e as áreas clientes. O UC é o contrato entre o provedor interno de TI e fornecedores externos. O OLA é um acordo entre o provedor interno de serviços de TI e outra área interna fornecedora de serviços necessários a TI. Quando elaborado um SLA os níveis de serviço devem levar em consideração o acordado nos SLAs e UCs.

O gerenciamento do Nível de Serviço é o processo que forma o vínculo entre o departamento de TI e os clientes.

Segundo OGCB (2001), o objetivo principal deste processo é assegurar a qualidade dos serviços em TI que são fornecidos, a um custo aceitável do negócio.

O Gerenciamento do Nível de Serviço gerencia a qualidade dos serviços em TI entregue conforme os acordos firmados entre os usuários e o departamento de TI.

O objetivo do Gerenciamento do Nível de Serviço é manter e melhorar a qualidade dos serviços através de um ciclo constante de acordos, monitoração, relatórios e melhoria dos níveis atuais de serviços.

10.2 GERENCIAMENTO DE DISPONIBILIDADE

As organizações estão se tornando cada vez mais dependentes sobre os serviços em TI, quando eles ficam indisponíveis, na maioria dos casos o negócio também sofre paralisação. Existe também um crescente aumento para todos os dias da semana, e em tempo integral, 24 horas por dia de disponibilidade dos serviços em TI.

É vital gerenciar e controlar a disponibilidade dos serviços em TI. O objetivo do Gerenciamento da Disponibilidade é conseguir um mapeamento claro dos requisitos do negócio relacionados com a disponibilidade dos serviços em TI e otimizar a capacidade da infra-estrutura para alinhar a estas necessidades.

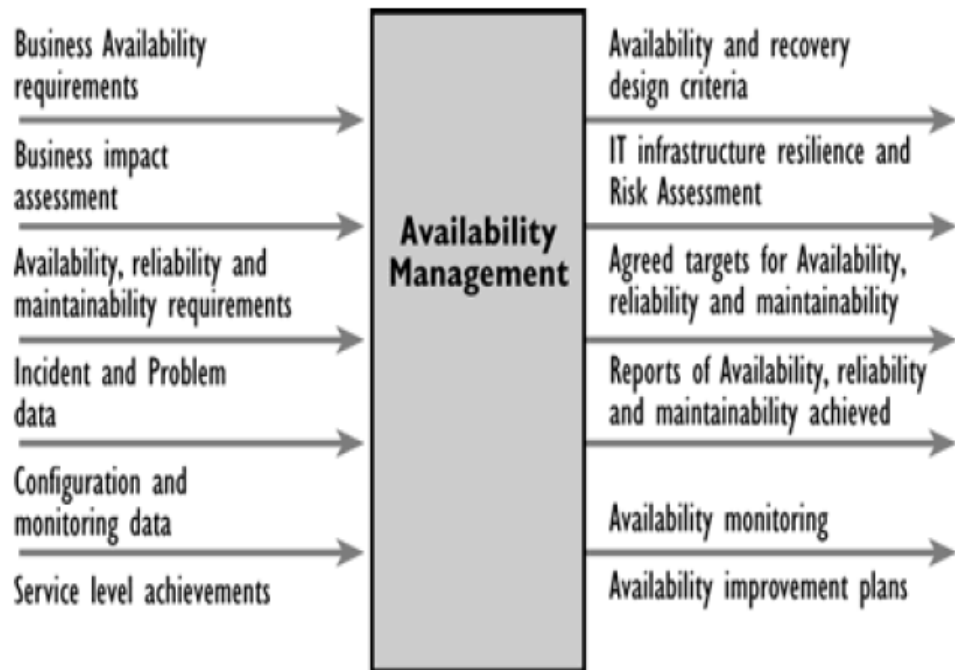


Figura 5. Entradas e saídas do Gerenciamento de Disponibilidade. Extraído de OGCB (2001).

A figura 5 exemplifica quais são as entradas e saídas do Gerenciamento de disponibilidade cobrindo o desenho, implementação, medindo e gerenciando a disponibilidade dos serviços. Mostra também a entradas e saídas do processo.

Para entrada: exigências de disponibilidade do negocio, uma avaliação de impacto no negocio, a disponibilidade ou confiança da infra-estrutura de TI, informações sobre as falhas dos serviços de TI, configuração e monitoramento dos dados que pertencem a cada serviço de TI e acordos de níveis de serviços definidos para o serviço prestado.

Para saída: disponibilidade e recuperação dos serviços, prevenção para minimizar impactos, acordos e objetivos de disponibilidade, relatórios de disponibilidade e plano para melhoria da disponibilidade.

Um bom exemplo é na Empresa Conecta que através de um software de gerenciamento é responsável por gerenciar e controlar a disponibilidade dos serviços prestados em TI e Telecom para seus clientes, os equipamentos são monitorados e gerenciados em tempo integral, e quando o seu espaço em disco chega a um determinado limite, é gerado um alarme informando que há algo de errado e uma solução é necessária.

10.3 GERENCIAMENTO DA CAPACIDADE

Segundo OGCB (2001), o processo de Gerenciamento da Capacidade foi desenhado para assegurar que a capacidade da infra-estrutura de TI esteja alinhada com as necessidades do negócio. O foco principal é entender e manter os níveis de entrega de serviços requisitados a um custo aceitável.

Através de investigação sobre as necessidades de capacidade, este processo irá gerenciar a capacidade necessária na infra-estrutura de TI para cumprir os requisitos do negócio.

O objetivo principal é entender os requisitos da capacidade do negócio e controlar entrega desta capacidade no presente e no futuro. O gerenciamento da Capacidade é também responsável por entender as vantagens potenciais que as novas tecnologias podem trazer para a organização.

10.4 GERENCIAMENTO DA CONTINUIDADE DOS SERVIÇOS

Poucos Gerentes vêem o Gerenciamento da Continuidade dos Serviços em TI como uma luxúria para a qual se não se direciona nenhum recurso. Cada vez mais desastres ocorrem freqüentemente, as causas de tais desastres são eventos como o incêndio, queda de raio, enchente, roubo, vandalismo, falta de energia ou ainda ataques terroristas.

Um plano de continuidade para o Negócio poderia salvar muitas empresas que foram afetadas por uma série de problemas ou ainda seus próprios negócios.

Cada vez que a disponibilidade ou desempenho de um serviço é reduzido, os usuários não podem continuar a trabalhar normalmente, é imprescindível estimar o impacto sobre a perda dos serviços em TI e se faça um Plano de Continuidade que assegure que o negócio sempre poderá continuar suas operações.

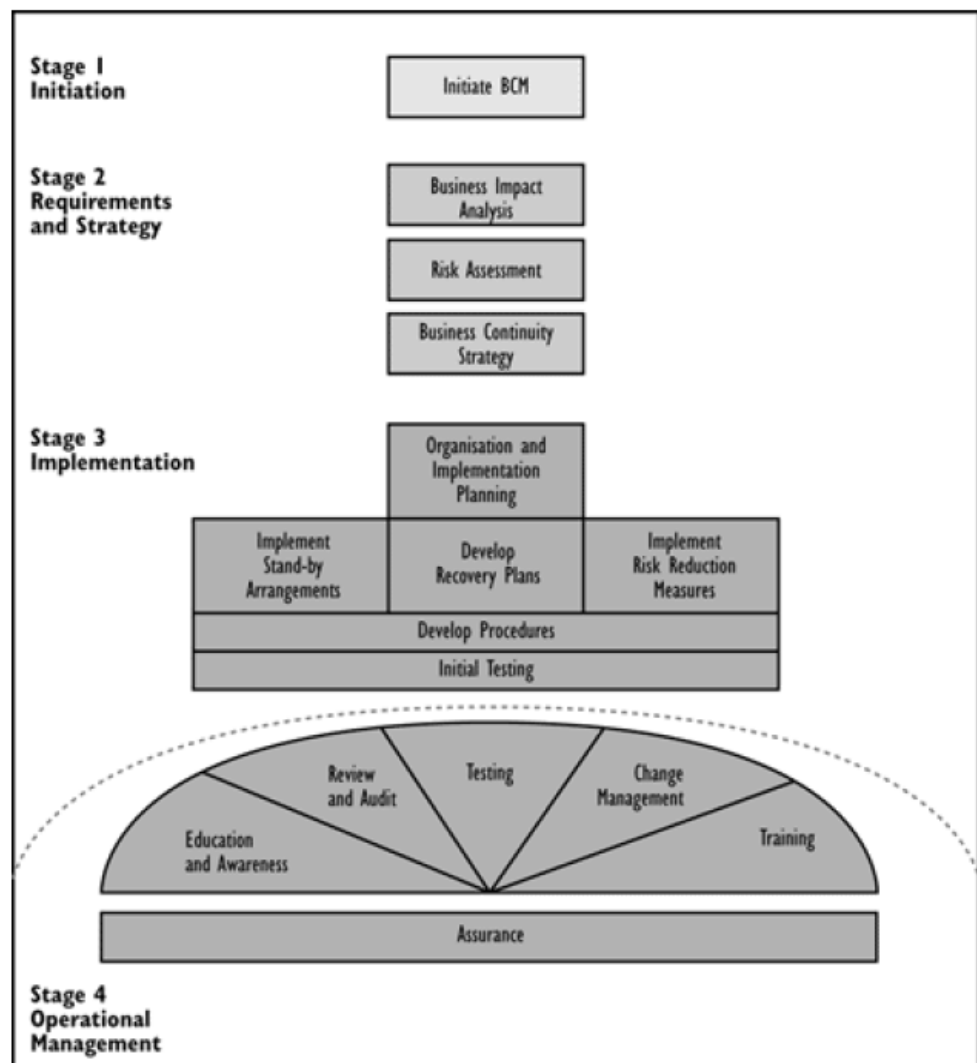


Figura 6. Processo de Gerenciamento de Disponibilidade. Extraído de OGCB (2001).

O objetivo do processo segundo OGCB (2001), é suportar de forma geral o gerenciamento da Continuidade de Negócio, assegurando que os requisitos técnicos de TI e facilidades de determinados serviços como sistema operacional, redes, aplicações, telecomunicações, suporte técnico e Central de Serviços possam ser recuperados dentro de escalas de tempo requeridas e acordadas.

A Figura 6 apresenta o Processo de Gerenciamento de Continuidade do Negócio, que é dividido em quatro etapas:

A primeira que é a fase de iniciação e depende em até que ponto as instalações de contingência foram aplicadas dentro da organização.

A segunda onde é feita a análise de impacto, avaliação de riscos e a estratégia da continuidade do negócio, determinam como organização sobreviverá a uma interrupção ou desastre na organização e seus custos envolvidos.

A terceira etapa que é o processo de implementação, uma vez que a estratégia estiver de acordo com o ciclo de vida da Continuidade do negócio, envolvendo se a TI a um nível detalhado, esta etapa implementa as medidas de redução de riscos, desenvolve os planos de recuperação, desenvolve procedimentos e empreende os testes iniciais.

E por fim, a quarta etapa que depois de ter implementado e planejados há uma necessidade de assegurar que o processo é mantido como sempre como parte do negócio, isto somente é alcançado com o gerenciamento operacional em educar e conscientizar os envolvidos treiná-los, rever regularmente os processos, estabelecer um programa de testes regularmente para assegurar os componentes críticos e obter a garantia da qualidade do Gerenciamento de Continuidade dos Serviços de TI.

10.5 GERENCIAMENTO FINANCEIRO

Segundo OGCB (2001), os serviços de TI são normalmente vistos como críticos no negócio ou organização. Nos últimos anos os negócios se tornaram mais dependentes de TI para realizar suas operações, conseqüentemente o número de usuários aumentou e a quantidade de gastos de TI.

Clientes e Diretores de Organizações são relutantes a gastar dinheiro para melhorar os serviços de TI se eles não tiverem um número claro dos custos envolvidos e os benefícios que isto pode trazer ao negócio. O gerenciamento Financeiro para serviços em TI pode tornar os custos mais claros, criando um método de cobrança e dando aos clientes uma idéia sobre a relação entre quantidade e preço.

O objetivo do processo de Gerenciamento Financeiro para os Serviços em TI para um departamento de TI interno deve ser: fornecer um custo efetivo para os gastos aplicados nos ativos de TI e recursos usados para fornecer os serviços em TI.

Em um ambiente corporativo pode haver ações que irão refletir no lucro e ações de marketing da organização.

O objetivo principal deste processo é o entendimento dos custos envolvidos na entrega de serviços em TI. Esta consciência dos custos melhora a qualidade de todas as decisões feitas em relação aos gastos. A cobrança dos custos do cliente é opcional.

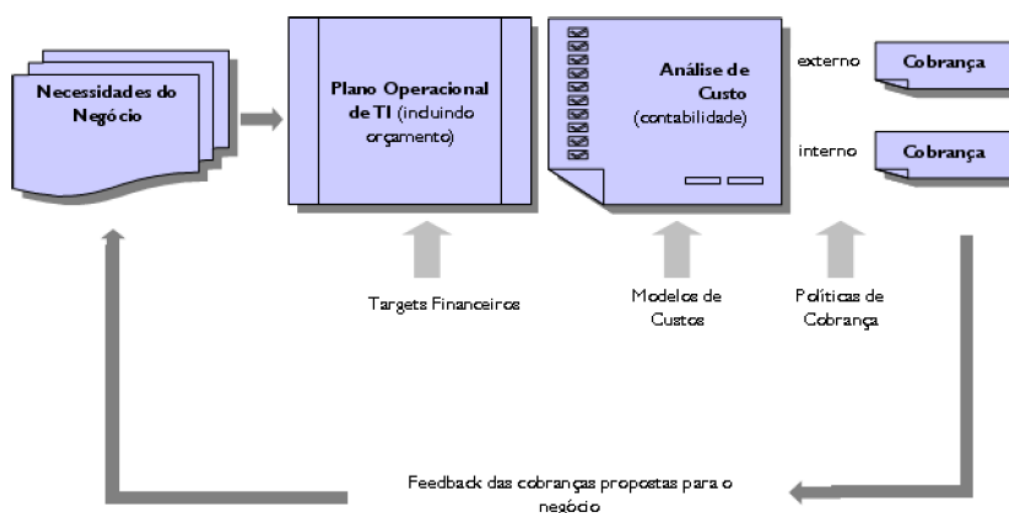


Figura 7. Exemplo de Processo de Gerenciamento Financeiro para Serviços em TI. Extraído da Empresa Conecta 2006.

A Figura 7 exemplifica o Processo Financeiro para Serviços que se baseia em três sub-processos:

Primeiro a elaboração do orçamento, que é o processo de prever e controlar os gastos em dinheiro dentro da organização e consiste de um ciclo de negociação periódica para criar orçamentos e monitoração diária dos mesmos. Assim assegura que os recursos em dinheiro necessários estão disponíveis para o fornecimento de serviços em TI e que durante o período do orçamento eles não serão extrapolados.

Segundo é a Contabilidade, que é um conjunto de processos que possibilita a organização contabilizar de que forma o dinheiro é gasto.

E Terceiro é a Cobrança, um conjunto de processos necessários para emitir as contas aos clientes dos serviços fornecidos a eles.

10.6 AUDITORIA DO PROCESSO DE GERENCIAMENTO

Sendo o ITIL uma referência, como garantir a implantação de forma efetiva e a sua sustentação ao longo do tempo? O problema da abordagem apresentada é que o ITIL não garante que os processos sejam realmente implementados nos seus requisitos mínimos. Deve existir na empresa uma Auditoria do tipo, um plano de qualidade que pudesse avaliar a qualidade do processo quanto à sua eficácia. Neste aspecto, normas de Certificação ou procedimentos podem complementar o ITIL. Existem ferramentas distintas no mercado que atuam com propósito semelhante, porém focando em o que fazer sob a ótica do ciclo de vida da Governança de TI e não em Gestão da Qualidade de Serviços.

11 ESTUDO DE CASOS

Na empresa 1, do segmento de Direito Penal foi feito um gerenciamento de Capacidade através de um software de monitoramento, por exemplo, um servidor gera alarmes informando memória muito alta, no entanto é identificado que é necessário adicionar mais memória no servidor, assim o administrador tem a informação correta do incidente gerado e consegue agir da forma correta.

Caso não tivesse boas praticas de gerenciamento, o problema poderia demorar a ser identificado e conseqüentemente solucionado, com isto causando um enorme transtorno e talvez prejuízos simplesmente pela paralisação ou até mesmo perda de informações.

Na empresa 2, do segmento de telecomunicações tem-se a interligação das filiais através de um link dedicado, um link na cidade A e outro na cidade B, que também estão interligadas por uma rede publica da empresa prestadora de serviço. A Empresa fornece serviços que opera 24 horas por dia e 7 dias da semana, inclusive pessoas treinadas trabalhando diariamente no caso de algum incidente.

Caso ocorra algum problema ou desastre na cidade A, o fluxo de ligações é direcionado para a cidade B. Apesar de menor quantidade de pessoas para o atendimento de duas cidades, todavia garantindo a disponibilidade do serviço, assim acontece também em caso de algum problema na empresa situada na cidade B, que também possui toda a contingência pronta e um planejamento para gerenciamento da rede em tempo integral.

Nos dois casos, se não ocorresse à prática de gerenciamento de rede e a presença de um plano de gerenciamento eficiente e eficaz, estas empresas teriam sérios problemas tanto de disponibilidade, confiabilidade e prejuízos conseqüentemente.

Ignorar a necessidade de gerenciamento pode trazer prejuízos incalculáveis dependendo dos acordos de Serviço (os SLAs), também devido a insatisfação e perda de clientes.

12 CONCLUSÃO

O gerenciamento da rede é fundamental para conseguirmos monitorar e controlar a operações da rede de modo a evitar possíveis falhas que tragam prejuízos maiores a Empresa ou as Operadoras em questão.

Os impactos podem ser desastrosos no caso de não ter o gerenciamento de rede ou mesmo ter, mas não ser gerenciado de maneira eficiente e eficaz. É necessário um comprometimento de todas as áreas envolvidas e de acordos pré-estabelecidos para facilitar todo o processo de Gerenciamento.

Uma Empresa que não coloca em prática técnicas de Gerenciamento pode ter prejuízo em sua aferição. Isto devido ao fato de não conseguir monitorar e controlar sua rede e ter uma informação precisa do desempenho da rede da Empresa. Consequentemente não tem parâmetros para avaliá-la e não consegue corrigir suas deficiências. Isto pode deixar de conquistar clientes e criar insatisfação nos clientes existentes.

Uma ótima base para gerenciamento dos processos de uma empresa, incluindo o gerenciamento da rede são os documentos ITIL. Um bom planejamento no projeto de Gerenciamento quantifica o tempo e o orçamento, aumentando as chances de sucesso do Negócio.

O gerenciamento de Mudanças esta relacionado com todas as disciplinas de entrega de serviços, conforme apresentado na seção anterior 9.3.

Todas as disciplinas trabalham juntas para fornecer Gerenciamento de Serviços ao negócio e aos usuários de sistema de TI. Os usuários podem ser funcionários dessa organização ou seus parceiros e clientes que cada vez mais usam serviços de TI diretamente, que faz aumentar a importância de um efetivo Gerenciamento dos Serviços.

O resumo do processo que compõe o ITIL para suporte de Serviços explica ilustrado que a Central de Serviço identifica o incidente, o incidente pode ser resolvido como incidente ou se tornar um problema.

É preciso identificar as causa do incidente para solucioná-lo com a maior brevidade possível, assim impactando menos nos serviços e negócio das organizações.

O Gerenciamento de rede é uma boa prática e deve ser encarado como uma ação que proporciona qualidade e lucro aos negócios e caso o gerenciamento não exista ou não venha a ocorrer corretamente vai influenciar no desempenho e resultado das organizações.

O crescimento das redes de computadores, juntamente com a integração de serviços como voz, vídeo e dados, introduzem a necessidade de um controle sobre o desempenho dos recursos, tornando-se de vital importância para garantia de qualidade dos serviços prestados. Assim, torna-se necessário lançar mão de recursos computacionais que proporcionem um gerenciamento mais eficaz e preciso.

Para conseguir gerenciar sistemas eficientemente e planejar inteligentemente um sistema de gerenciamento de redes, o profissional necessita conhecer os conceitos fundamentais e as tecnologias de gerência de redes, tornando possível atingir os seus objetivos, monitorando e controlando os elementos da rede (sejam eles físicos ou lógicos) e assegurando um determinado nível de qualidade dos serviços oferecidos aos usuários.

Concluindo, a gerência de redes está associada não somente ao controle de atividades e ao monitoramento do uso de recursos da rede, como também às necessidades atuais e futuras de toda a infra-estrutura da rede, consoante as necessidades estratégicas de seus usuários. As atividades da gerência de redes são complexas e interdependentes, requerendo um fluxo de informações eficaz e contínuo para sua realização.

REFERÊNCIAS

CAMURUGY, Patricia. ITIL na Governança de TI. 2005. Disponível em: http://www.timaster.com.br/revista//artigos/main_artigo.asp?codigo=984. Acesso em: 19 Nov. 2008.

DERFLER J.R, Frank J; FREED, Les. *Como Funcionam as Redes*. Tradução: Eduardo Simom. Ilustração: Michael Troller. 3.ed. [S.I]: Quark, 1993. 217p.

FRY, Malcolm. *Building a Case for Pursuing ITIL Best Practices in your Organization*. Sunnyvale, USA: Remedy, 2003.

GALLO, Michael A; HANCOCK, William M. *Comunicação entre Computadores e Tecnologias de Rede*. Tradução Técnica: Flávio Soares Corrêa da Silva, Márcio Rodrigo de Freitas Carneiro, Ana Cristina Vieira de Melo. São Paulo: Pioneira Thomson Learning, 2003. 673p.

GUERRAOUI, R; SCHIPER, A. *Fault-Tolerance by Replication in Distributed Systems*. International Conference on Reliable Software Technologies, Springer Verlag, 1996.

HANRRINGTON, D; PRESUHN, R; WIJNEN, B. *An Architecture for Describing SNMP Management Frameworks*: RFC 3411, 2002.

ITSMF, IT Service Management Forum. *IT Service Management, an Introduction*. Sd. Reino Unido: ITSMF, 2001.

LAUDON, Kenneth C; LAUDON, Jane P. *Management Information Systems: Managing the Digital Firm*. 7th ed. New Jersey: Prentice Hall, 2002. 549p.

LEINWAND, Allan; CONROY, Karen Fang. *Network Management: Pradical Perspective*. 2th ed. California: Unix and Open Systems, 1999.338p.

LOPES, Raquel V; SAUVÉ, Jacques P; NICOLLETTI, Pedro S. *Melhores Práticas para Gerência de Redes de Computadores*. 1.ed. Rio de Janeiro:Elsevier, 2003. 378p.

MAGALHÃES, Ivan Luizio; PINHEIRO, Walfrido Brito. *Gerenciamento de Serviços de TI na Prática: Uma abordagem com base na ITIL*. São Paulo: Novatec, 2007.

MAURO, D; SCHMIDT, K. *Essential SNMP*. 2.ed. O Reilly, 2005. 460p.

OGCa, Office of Government Commerce. *Service Delivery*. Londres, Inglaterra: The Stationary Office, 2001.

OGCb, Office of Government Commerce. *Service Support*. Londres, Inglaterra: The Stationary Office, 2001.

SOARES NETO, Vicente. *Rede de Dados Teleprocessamento e Gerência de Redes*. São Paulo: Érica, 1990. 200p.

Stallings, W. *Snmp, Snmpv2, Snmpv3 and Rmon: The Practical Network Management*. 2.ed. Reading, Addison-Wesley, 1996. 478p.