2
Estudo de Caso

O gerenciamento de serviços é um fator crítico para a organização em análise, os processos devem garantir os acordos de níveis de serviços estabelecidos com os clientes. Destarte, a atividade de monitoração do ambiente de TI é imprescindível. A empresa investiu muito em ferramentas para manter um ambiente de monitoração eficiente, mas nesse momento a preocupação maior é com o tratamento dos alarmes e com mecanismos que possam facilitar essa tarefa.

Uma nova tendência de mercado vem crescendo para o ambiente de monitoração, trata-se do centro de comando. O centro de comando deve ter autonomia suficiente para tratar em primeiro nível os alarmes de monitoração, conseqüentemente, minimizando o tempo de indisponibilidade dos serviços e priorizando os mais críticos. Em nosso cenário, o CORS representa o centro de comando.

Entretanto, para desempenhar essa atividade, o centro de comando precisa contar com um sistema de gerenciamento de conhecimento eficiente que indique o que deve ser feito para tratar qualquer tipo de alarme. Ao estudar brevemente o ambiente atual, constatamos que o sistema de gerenciamento de conhecimento usado pelo CORS tem algumas deficiências.

Atualmente a rede interna corporativa da organização em análise possui mais de 100 mil computadores e 6 mil servidores espalhados por 28 países. Para garantir excelência operacional e atender os membros da organização é necessário manter uma infraestrutura de TI gigantesca e extremamente complexa. Neste cenário, o gerenciamento dos serviços de TI é uma tarefa imprescindível e desafiadora.

O gerenciamento de serviços é uma estratégia orientada a processos para a entrega de serviços em TI, com foco no cliente, que atende ao conjunto de metas de custo e performance estabelecido em parceria com os clientes das linhas de negócio e incorporado aos acordos de níveis de serviço (*SLA- Service Level Agreements*) e acordos de níveis operacionais (*OLA – Operational Level Agreements*) [Central Computer & Telecommunications Agency].

O gerenciamento de incidentes é o processo dentro do gerenciamento de serviços responsável por monitorar o ambiente de TI no sentido de obedecer aos níveis de serviço pré-determinados e escalar corretamente os incidentes dentro do processo de entrega do serviço à medida que eles surgem. O ambiente de monitoração da empresa em análise pode ser resumido na figura 2.

O ambiente de monitoração é composto por muitos sistemas, cada um com sua respectiva responsabilidade, isto é necessário para garantir o nível de serviço adequado para os clientes. A figura 2 mostra os principais sistemas de monitoração para o ambiente de TI, note que os sistemas responsáveis pela monitoração das telecomunicações e dos elementos de redes não fazem parte deste estudo e não foram relacionados na figura 2. Cada nuvem representa um sistema, entretanto, não cabe entrar nos detalhes das complexas arquiteturas de cada sistema. As setas indicam os sentidos dos fluxos de dados.

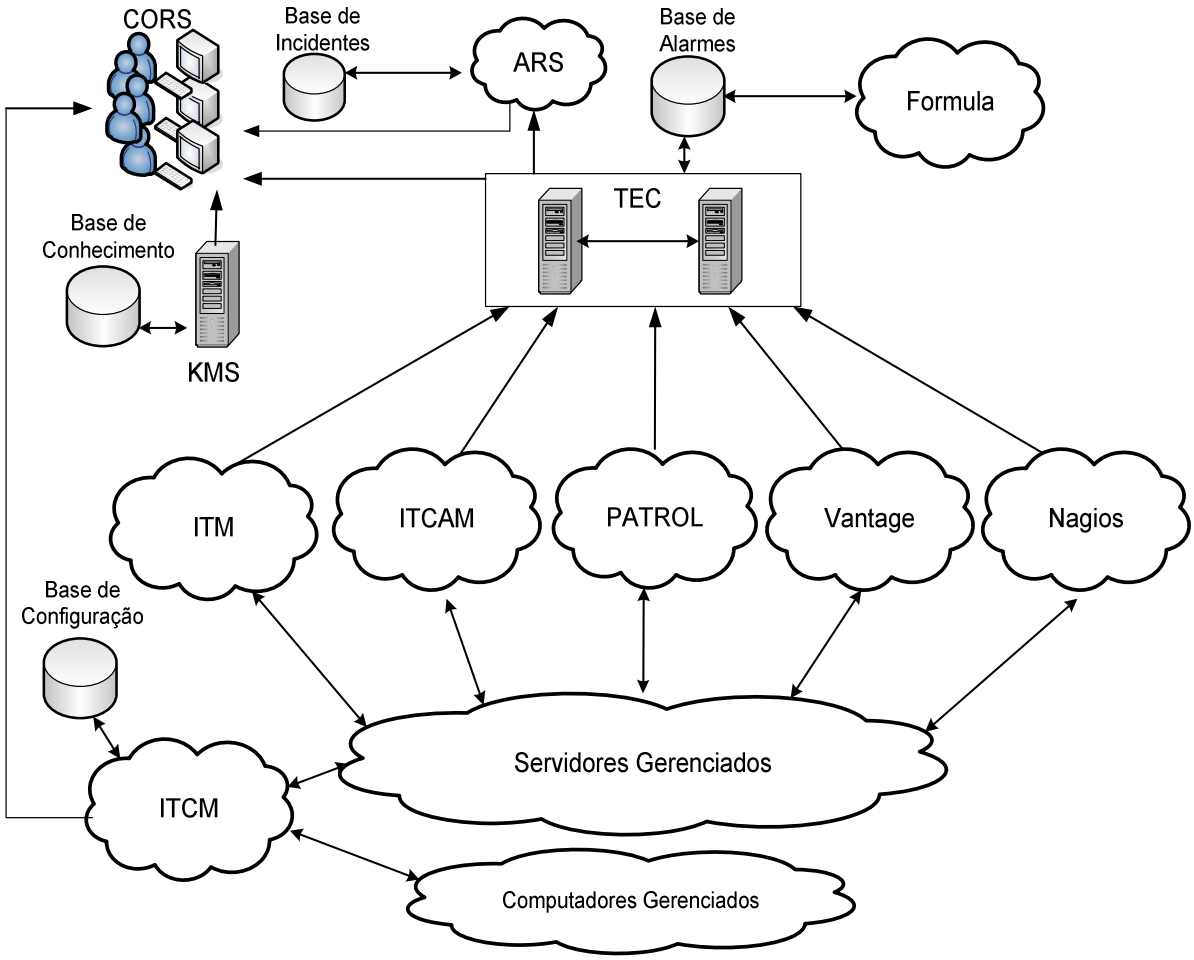

Figura 2 – Principais Componentes do Ambiente de Monitoração.

Apenas como referência, a figura 3, nos dá uma visão mais ampla sobre os sistemas de gerenciamento de TIC usados na empresa. Alguns serão descritos em seguida.

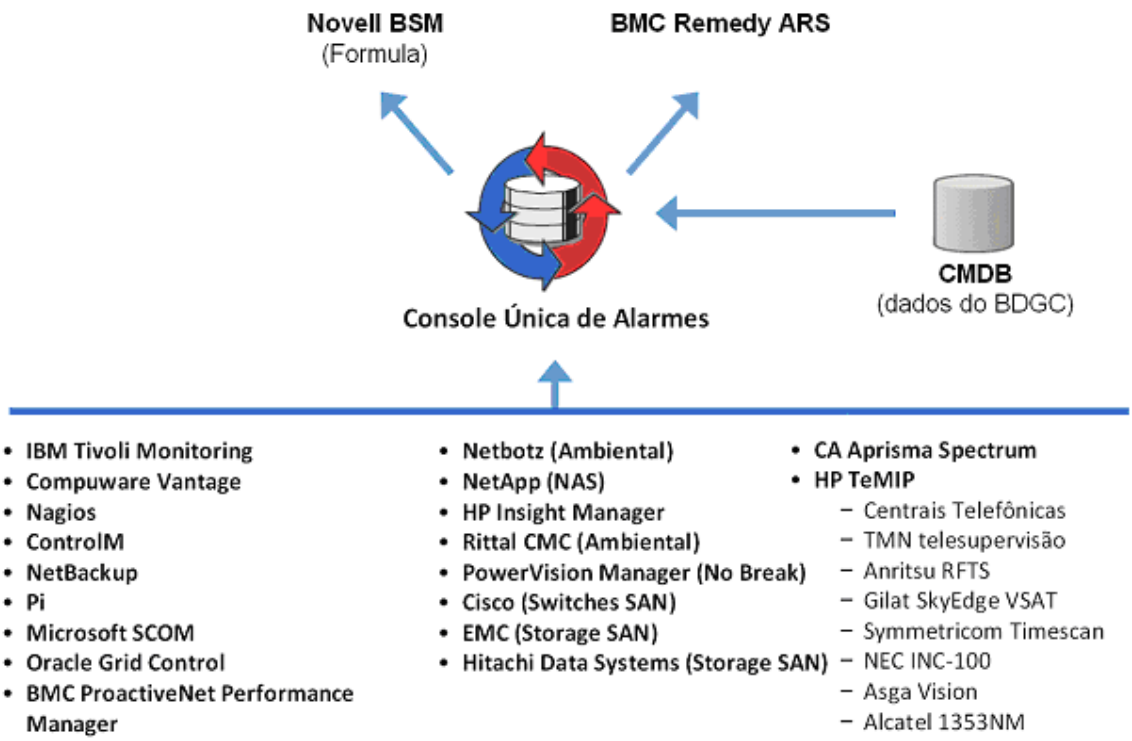

Figura 3 – Outros componentes do Ambiente de Monitoração.

O *ITM – IBM Tivoli Monitoring* é o software responsável pelo monitoramento de recursos dos sistemas, detecta gargalos e problemas potenciais, além de recuperar-se de situações críticas. Monitoração de processador, memória, disco, filesystems e processos são exemplos das tarefas executadas pelo ITM. Na organização, o ITM monitora todos os servidores em produção, cerca de 6 mil, independente da plataforma e do sistema operacional. Para que isto ocorra é necessária a instalação de um agente no servidor gerenciado.

O *Patrol – BMC Performance Manager* é o sistema responsável pela monitoração de todos os bancos de dados da organização, da ordem de milhares. O Patrol monitora bases de diferentes fabricantes, incluindo monitoração de transações, tabelas e instancias.

O *ITCAM – IBM Tivoli Composite Application Manager* é o sistema responsável por monitorar a disponibilidade e o desempenho das aplicações Web. Neste caso não é necessário a instalação de nenhum agente no servidor gerenciado,

o ITCAM atua como um robô, simulando a navegação de um usuário comum. Atualmente, algumas centenas de aplicações são monitoradas.

O *Nagios* [1] é um software de código aberto distribuído sob licença GPL. Na organização, ele é responsável pela monitoração de disponibilidade de servidores e serviços, através da verificação de portas TCP. Assim como o *ITM* este sistema monitora todos os servidores em produção, mas sem necessidade de instalação de agente no servidor gerenciado.

O *Vantage*, do fabricante Compuware, é responsável pela monitoração de servidores Web (*Weblogic, Websphere, Apache, IIS*...) e suas respectivas aplicações e transações. Este software faz o monitoramento da experiência final do usuário final.

Ao detectar qualquer comportamento fora do normal, os sistemas de monitoração, citados acima, enviam um evento para a *TEC* (*Tivoli Enterprise Console*). A *TEC* é um sistema de gerenciamento de eventos baseado em regras e responsável por receber e processar os eventos de monitoração. Dependendo da regra associada ao evento recebido, a *TEC* executa alguma ação. Um evento do tipo *FATAL*, por exemplo, indica a indisponibilidade de algum servidor, nesse caso a *TEC* exibe essa informação para o CORS (Centro de Operação de Redes e Sistemas) e gera um incidente no ARS (*Action Request System).* A figura 4 ilustra alguns alarmes classificados como *CRITICAL* na console da *TEC.*

[1] Nagios – www.nagios.com

File Edit Options Selected Automated Tasks Help

Working Queue

0 275 18 2 653 52

Status	Sever...	Hostname	Me...	R...	Message	Class
Open	Critical	Removido	RIO	0	Consumo da CPU 0 critica	TMW_ProcessorBusy
Open	Critical	Removido	RIO	0	Servico SAP R/3 - INTERNACIONAL/UN-USA indisponivel.	BSM_Alarme_Servico
Open	Critical	Removido	RIO	0	Servico SAP R/3 - Sistema xx ;SAP Produ??o PAI-Houston) indisponivel.	BSM_Alarme_Servico
Open	Critical	Removido	RIO	0	Removido - Instancia: Removido - Instancia indisponivel	PATROL_ORACLE_AVAILABILIT
Open	Critical	Removido	SE	0	Espaco disponivel no file system insuficiente - /var/spool/samba	LowPercSpcAvail
Open	Critical	Removido	RIO	0	Consumo da CPU 0 critica	TMW_ProcessorBusy
Open	Critical	Removido	RIO	0	Consumo da CPU 1 critica	TMW_ProcessorBusy
Open	Critical	Removido	RIO	0	Consumo da CPU 3 critica	TMW_ProcessorBusy
Open	Critical	Removido	RIO	0	Consumo da CPU 5 critica	TMW_ProcessorBusy
Acknowledged	Critical	Removido	BC	0	Espaco no drive C: abaixo de 900 Mb	TMW_LowLogicalDiskSpaceMb
Open	Critical	Removido	RIO	0	Espaco no drive D: abaixo de 6 %	TMW_LowLogicalDiskSpace
Open	Critical	Removido	ES	0	Servico Monitoring Agent for Windows OS - Primary (KNTCMA_Primary) para	TMW_ServicesStopped
Open	Critical	Removido	RIO	0	CRITICO - Servidor: Removido Particao: Removido Removido - Valor 95	PATROL_FILESYSTEM
Acknowledged	Critical	Removido	RIO	0	Consumo da CPU 0 critica	TMW_ProcessorBusy
Acknowledged	Critical	Removido	RIO	0	Servico National Instruments LXI Discovery Service (niLXIDiscovery) parado	TMW_ServicesStopped

Figura 4 – Console da TEC*.

*Alguns dados foram removidos atendendo a política de segurança da informação da empresa.

O *ARS – Action Request System* registra todo o ciclo de vida de um incidente. Todas as informações sobre o tratamento do incidente são registradas no ARS, desde sua abertura até seu fechamento.

O *ITCM – IBM Tivoli Configuration Manager* não é diretamente responsável pela monitoração de infraestrutura de TIC, mas faz parte do processo de gerenciamento de configuração que serve de base para todos os outros processos de gerenciamento de infraestrutura de TIC, inclusive para o gerenciamento de incidentes. Uma das funções deste sistema é o de manter um inventário de hardware e software atualizado de todos os computadores gerenciados. O *ITCM* gerencia não somente os servidores, mas todos os computadores da organização.

O *Formula* é o *BSM – Business Service Management* da Novell, este software fornece uma visão de serviço, responsável por gerenciar os acordos de nível de serviço estabelecidos com os clientes. Um serviço pode ser composto por elementos de rede, bancos de dados e servidores de aplicação, a indisponibilidade de qualquer um desses componentes causa indisponibilidade do serviço. Quando a TEC recebe um alarme de indisponibilidade de algum componente deste serviço, o Formula é responsável por gerenciar o tempo de indisponibilidade do serviço e comparar com o *SLA* estabelecido com o cliente para este serviço.

A base de conhecimento é gerenciada pelo sistema de gerenciamento de conhecimento do estudo de caso. Esse sistema é uma aplicação Web conhecida como Portal de Operação e Infraestrutura. Neste portal os especialistas de cada ambiente registram os diversos conhecimentos, dentre eles, os conhecimentos necessários para o CORS (Centro de Operação de Redes e Sistemas) tratar os alarmes correspondentes a cada um dos serviços. O sistema de gerenciamento de conhecimento atual será abordado no item 2.1.

O CORS é a equipe responsável pela análise dos alarmes de monitoração. Esta equipe está presente em cinco regionais diferentes, trabalha em turno e atua 24 horas, todos os dias da semana. Durante a análise do evento, para decidir que ação deve ser tomada, o CORS, além de verificar as informações da TEC, também pode consultar as informações de configuração do servidor com alarmes ativos na base do ITCM e as informações sobre o tratamento de alarmes na base de conhecimento.

2.1. Sistema Atual

Nesta seção, o sistema de gerenciamento de conhecimento usado na empresa será um pouco mais detalhado. Na fase de análise, com base nas informações dessa seção, as possíveis limitações do sistema serão identificadas e estudadas.

O sistema de gerenciamento de conhecimento do estudo de caso é conhecido como ‘Portal de Operação e Infraestrutura’ usado por toda gerência geral de infraestrutura de TIC da empresa: cerca de 5.500 pessoas distribuídas por dezenas de países. Os especialistas das diversas áreas usam o sistema para cadastrar conhecimentos sobre seus ambientes, dentre eles, os conhecimentos relativos ao tratamento dos alarmes consultados pelo CORS.

Para tratar um alarme, o CORS pode precisar dos dados de configuração do servidor tais como: o sistema operacional ou aplicação, a localização do servidor como país, cidade ou CPD, dos detalhes do alarme como horário, descrição ou métricas de monitoração. Por exemplo: ao receber um evento de queda do processo “*gateway*”, de um servidor com a aplicação *Tivoli*, com sistema operacional Linux, em Okinawa - Japão, às 2:00 horas da manhã (horário de Brasília), o CORS consulta a base de conhecimento e aprende que nesta situação deve acionar um

servidor de contingência (e como deve fazer isso) e que também deve acionar um especialista de sobreaviso de uma determinada equipe caso a situação não se normalize. No exemplo acima, o CORS precisou consultar a base de conhecimento, a base de alarmes e a base de configuração para tomar uma ação de primeiro nível.

O sistema de gerenciamento de conhecimento do estudo de caso não é integrado com o sistema de tratamento de alarmes, a *TEC* e o sistema de gerenciamento de configuração, o *ITCM*. Como o operador perde um tempo considerável procurando informações ou conhecimentos em todos esses sistemas para tratar os alarmes recebidos, o tempo de indisponibilidade dos serviços aumenta.

Freqüentemente, com informação e conhecimento limitados, ausentes ou não encontrados no sistema de gerenciamento de conhecimento, o CORS, por não saber como tratar determinados alarmes, acaba se tornando um mero intermediário e apenas repassa os alarmes recebidos para os especialistas responsáveis pelo servidor/serviço impactado. Neste caso, o CORS precisa consultar, no mínimo, o responsável pelo serviço/servidor alarmado, o que é muito indesejável, pois aumenta o custo de manutenção e o tempo de indisponibilidade dos serviços. Se o serviço for crítico e causar impactos para o negócio a situação é ainda pior.

Em alguns casos graves, o operador não encontra nenhuma informação sobre o alarme recebido, nem mesmo o especialista responsável nesta situação e assim um evento crítico deixa de ser tratado ou encaminhado pelo CORS.

A figura 5, abaixo, ilustra a navegação pelo sistema de gerenciamento de conhecimento do estudo de caso. A navegação é hierárquica, o círculo vermelho destaca o caminho percorrido para chegar aos procedimentos da equipe de Monitoração, onde é necessário passar antes pela gerência geral A, pela gerência B e pelo setor C. O quadrado azul destaca a relação de procedimentos ativos exibidos por data e título e organizados por categoria. O procedimento “Monitoração *Patrol* para o sistema *BDXYZ*” é o único dentro da categoria BMC/PATROL.

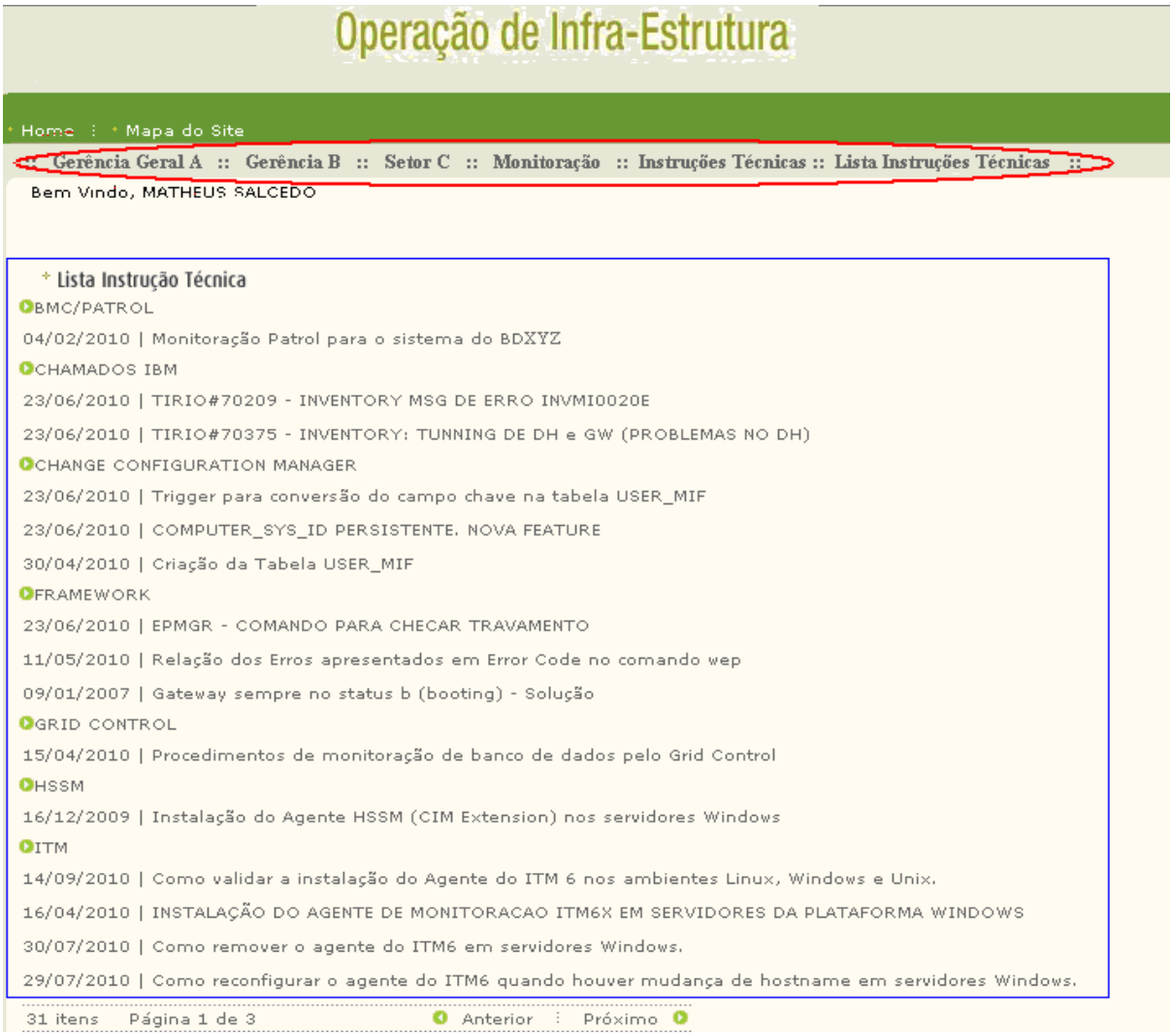

Figura 5 – Navegação no Sistema de Gerenciamento de Conhecimento Atual.

Os procedimentos têm um ciclo de vida, eles podem passar por diferentes status, entre eles: em criação, em aprovação, em revisão, expirado e ativo. Os procedimentos devem ser revisados em determinado período de tempo, caso contrário expiram e ficam indisponíveis para consulta. Todo novo procedimento criado por um autor deve ser aprovado pelo líder da equipe para se tornar ativo.

A figura 6, abaixo, ilustra outra possibilidade de procurar um determinado procedimento através da função de busca. No exemplo ilustrado o usuário fez uma busca sintática pela palavra ‘itm’. Observe que o último procedimento parece útil para o CORS no tratamento de alarmes: “Tratamento de alarmes do servidor xxxx – e a instancia yyyy”.

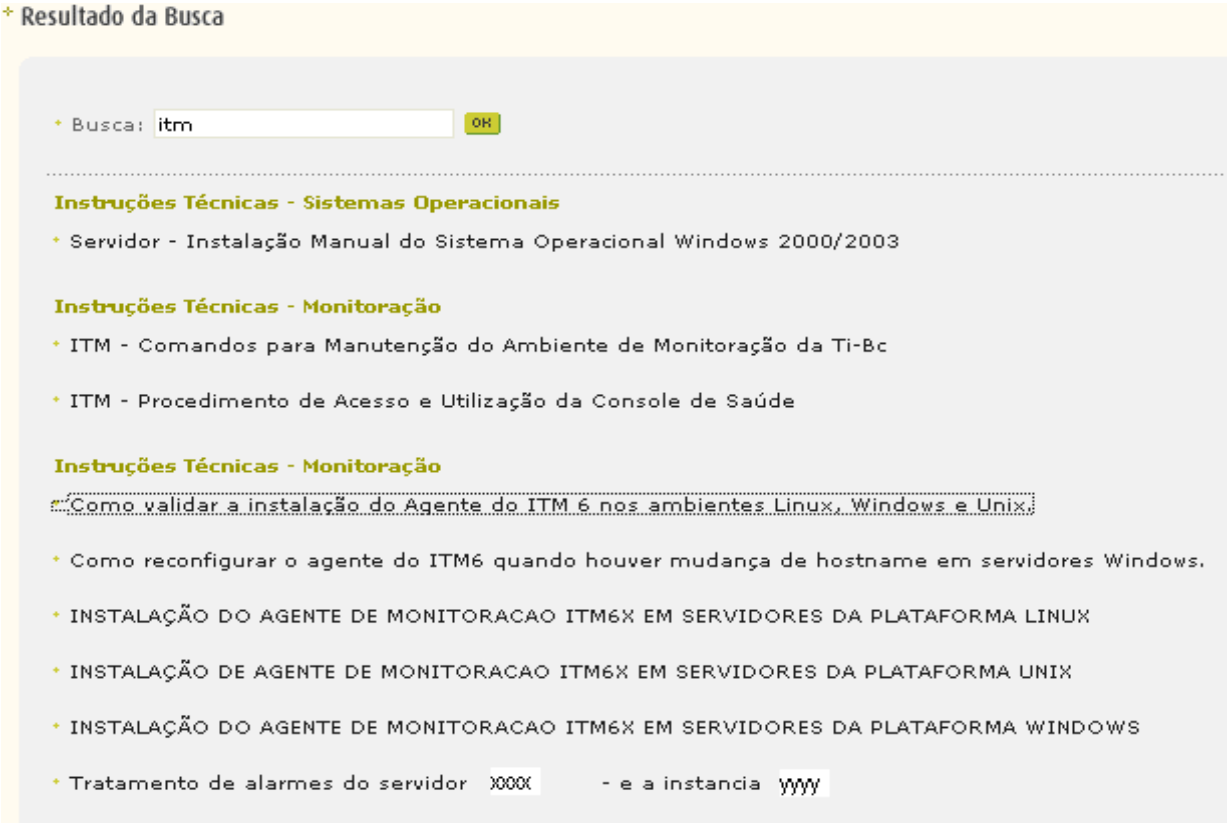

Figura 6 – Busca no Sistema de Gerenciamento de Conhecimento Atual.

A figura 7, abaixo, mostra o procedimento “Tratamento de alarmes do servidor xxxx – e a instancia yyyy” que orienta o CORS a tratar alarmes de um servidor de banco de dados. Neste caso, o CORS deve executar um *script* para normalização do ambiente e acompanhar o status do alarme, se o incidente não for resolvido em determinado período de tempo, o CORS deve acionar o responsável pelo SGBD (no caso a equipe responsável pelos bancos *Oracle*) para solucionar o problema e também notificar a equipe de Monitoração responsável pela aplicação. O cabeçalho do procedimento possui dados relacionados ao procedimento, como: data de criação, autor, data de modificação, editor, data de expiração e versão. O cabeçalho também indica que existe um pedido de revisão para o procedimento.

Tratamento de alarmes do servidor xxxx - **instancia** yyyy

Data de criação :	23/03/2009
Criado por :	LEONARDO
Data da última modificação :	24/03/2009
Último a modificar :	URSULA
Expira em :	06/01/2010
Versão Atual :	2
Estágio :	(Existe um pedido de revisão para esta Instrução)

1. Objetivo
Orientar ao CORS de como devem ser tratados os alarmes do servidor xxxx e da Instancia yyyy

2. Pré-Requisitos
N/A

3. Aplicação
Equipe de Monitoração e Suporte ORACLE

4. Documentos de Referência
n/a

5. Definições
n/a

6. Objeto

Os alarmes registrados no ARS para o servidor XXXX, instância YYYY devem ser tratados conforme a seguir:
1- O operador do CORS deve localizar o servidor XXXX na TEP (Tivoli Enterprise Portal).
2- Selecionar o servidor XXXX e clicar em "Run Action..."
3- Selecionar e executar o script "reiniciar_yyyy.sh"
4- Aguardar 10 minutos e caso o alarme não normalize, acionar a equipe Oracle e notificar a equipe Monitoração

7. Registros

Nome	Recuperação	Armazenamento	Retenção	Proteção	De
IBM Tivoli DataWareHouse	Instalacão de produto	Servidor Data Warehouse	6 meses	senha de sistemas	6 r

Figura 7 – Exemplo de Procedimento no Sistema de Gerenciamento de Conhecimento Atual.