GESTÃO DE HARDWARE E SOFTWARE EM AMBIENTE CORPORATIVO

Luciano B. Buzzacaro

Graduado em Sistemas de Informação, Especialista em Desenvolvimento para Ambiente Internet, UTFPR - Universidade Tecnológica Federal do Paraná – Campus Pato Branco.

lucianobb@sanepar.com.br ;

Resumo – Atualmente, a área de Tecnologia da informação e comunicação (TIC) se faz uma necessidade irremediável em qualquer ambiente corporativo ou não, independente do ramo de atuação da empresa. Dessa forma, é muito importante a existência de setores responsáveis pela gestão dos recursos de TIC. É necessário que exista planejamento para administrar o parque tecnológico da empresa. A gestão dos recursos e das ferramentas de hardware e software interfere, diretamente, em fatores como segurança das informações e segurança da rede corporativa. Existe ainda, o fator humano que participa, efetivamente, da utilização do hardware e software da empresa, interferindo no contexto da política de qualidade, haja vista, a necessidade de comprometimento com o uso consciente dos recursos tecnológicos e das informações corporativas.

Palavras Chave – Tecnologia da Informação, TIC, gestão de software, gestão de hardware, segurança da informação.

GESTÃO DE HARDWARE E SOFTWARE EM AMBIENTE CORPORATIVO

1. INTRODUÇÃO

Com o crescimento atual do setor de tecnologia da informação e comunicação (TIC), as empresas corporativas necessitam muito que suas equipes de informática, estabeleçam critérios e procedimentos normativos em busca de padronização interna, tanto de hardware quanto de software, como forma de minimizar os problemas de heterogeneidade e outras incompatibilidades que, comumente, causam muita dor de cabeça e aumentam muito o custo de suporte ao usuário da equipe de TIC da empresa. De forma que, é extremamente importante estabelecer diretivas e procedimentos de segurança, que garantam a integridade das informações de relevância armazenadas em microcomputadores (*desktop*s e *laptops*) dos usuários, ou seja, aqueles dados que não são armazenados nos servidores ou *mainframe* da empresa e que na maioria das vezes, ou poderia ser dito quase em sua totalidade, não passam por rotinas de backups diários, diferentemente do que acontece nos servidores, onde as cópias de segurança são priorizadas. O objetivo é proteger essas informações das diversas ameaças virtuais e físicas, a fim de garantir a continuidade dos negócios, a integridade e a disponibilidade dos recursos e dos dados.

O fator humano ou *peopleware* também tem participação bastante efetiva na utilização do hardware e software da empresa, interferindo diretamente no contexto da política de qualidade, visto a necessidade de comprometimento com o uso consciente do parque tecnológico da corporação.

Da mesma forma que cabe ao setor de TIC da empresa: pesquisar, selecionar, homologar e adquirir as melhores ferramentas e equipamentos, cabe também a ela, a tarefa de buscar a minimização de custos com a área de tecnologia, seja buscando equipamentos de hardware mais baratos, mas que não comprometam a qualidade, seja buscando ferramentas de

software gratuito ou de menor custo, mas que não comprometam a segurança dos dados da empresa, disponibilizando as ferramentas de hardware e software necessárias, para a realização das tarefas administrativas, bem como, o armazenamento das informações e estabelecer a especificação de configurações padrões nos equipamentos de informática da empresa.

2. FUNDAMENTOS DO ESTUDO

As empresas, independente da área de atuação, têm de forma crescente potencializado o uso amplo e intensivo de informações e suas tecnologias, com o objetivo de desenvolver modelos de negócio, sugerir modelos organizacionais e de integração de cadeia de valor física e virtual, aperfeiçoar processos de implementação e gestão de tecnologia de informação para melhorar os processos, e desenvolver ferramentas e técnicas de análise qualitativa e quantitativa de grandes volumes de informações. Inserido nesse contexto, o estudo de certos fatores como a análise de custo *versus* benefícios, que interferem direta ou indiretamente no funcionamento das atividades da empresa, se tornam importantes ferramentas de decisão.

Conforme afirma GRAEML

> Considerando-se os efeitos decorrentes da transformação ocasionada pela informatização e o fato da grande dificuldade em mensurar o retorno sobre o investimento em TI, a gestão da implementação de recursos de informática deve visar os benefícios e não a diminuição de custos decorrentes. Um primeiro passo para uma decisão acertada é ter consciência de que os benefícios advindos do investimento em TI não estão diretamente ligados ao próprio investimento, mas ao uso que é feito dela. (GRAEML, 2000)

Para bem conduzir a administração dos recursos de informática os gestores devem reconhecer os fatores importantes na sua administração e implementação, enfocando o gerenciamento da nova cultura, das mudanças, das tendências e das transformações provocadas pela utilização das TICs no âmbito global da empresa.

Verdadeiramente, as TICs trouxeram mudanças de paradigma que precisam ser assimiladas nas corporações conforme REZENDE (2003),

> a corrida pela produtividade requer a substituição, onde possível, do papel e tinta por sinais eletrônicos, o que nos leva aos diversos planos de análise desta possibilidade. Em cada um desses planos, listados abaixo, há que se considerar os enfoques de viabilidade e de risco, para alcançarmos o significado do rito que transmuta bits em verdades presumidas.
>
> Em relação à viabilidade:
>
> Plano técnico: O advento das redes de comunicação de hierarquia aberta e topologia escalável, que aqui chamaremos abreviadamente de redes abertas, tais como a Internet e a telefonia móvel, viabilizou, do ponto de vista semiológico, a substituição do documento em papel pelo documento eletrônico, tornando os canais de comunicação digital ubíquos;
>
> Plano econômico: Nos casos em que os custos para a disseminação das respectivas tecnologias, a saber, as de armazenamento, identificação, proteção, transporte, apresentação, controle e interoperação, são compensados por ganhos de eficiência e de escala, a substituição se torna racional na lógica econômica.
>
> Plano jurídico: O legislador deve ser acionado para regulamentar novas práticas comunicativas na medida em que se consolidem como socialmente aceitáveis, para adequá-las aos preceitos normativos que regem os costumes, em consonância com aqueles já sedimentados nas diversas jurisprudências, se tais novas práticas não são alcançáveis pela Hermenêutica.

Visto a importância que a área de TIC alcançou no cenário mundial, seja no ramo industrial, empresarial, comercial, financeiro ou outro qualquer, tornou-se uma necessidade global e inerente às necessidades básicas para o funcionamento de qualquer negócio que trabalhe inserido no meio globalizado. “A TI passou a ser o quarto principal recurso disponível para os executivos, depois das pessoas, do capital e das máquinas.” (GRAEML, 2000)

A partir do momento que as empresas passam a ser dependentes das TICs para que seus negócios fluam de forma

harmônica, se faz necessário o estudo aprofundado dos critérios e procedimentos de utilização do ambiente informatizado da empresa e estes devem ser observados de forma sumária. Devem ser utilizados somente para atender as necessidades de negócio da corporação, sendo o seu uso limitado ou proibido para quaisquer outras atividades. Esses procedimentos passam a ser necessários para segurança e proteção dos dados, a fim de garantir a integridade das informações de relevância para os negócios da empresa, informações estas armazenadas em meios eletrônicos. Além disso, é preciso acompanhamento e gestão do parque tecnológico para garantir a manutenção e a renovação periódica dentro das necessidades de utilização dos recursos de hardware e software, garantindo assim a eficiência dos serviços que dependem dos recursos de TIC. É nesse ponto que infere o estudo de caso que segue.

3. O ESTUDO DE CASO

O estudo realizado apresenta observações das normas, instruções técnicas e de apoio baseadas na política de qualidade adotada pela Companhia de Saneamento do Paraná – SANEPAR, a qual apresenta uma metodologia de padronização de ferramentas de hardware e software, a fim de facilitar o trabalho de gerenciamento da Unidade de Serviço de Tecnologia da Informação (USTI), no que diz respeito ao parque de TIC da empresa. A USTI é o setor da SANEPAR responsável por oferecer todo suporte em TIC para os demais setores da Companhia. No decorrer do artigo será utilizada a expressão “unidade gestora de TIC” ou “unidade de serviços de TIC” para generalizar o setor interno que atende a todos os serviços de TIC da empresa. Vale ressaltar que em cada empresa existem formas particulares para determinar a divisão em grupos, setores, equipes, unidades, departamentos ou outra expressão que determina o foco de atuação interno, sendo que todos esses setores juntos é que efetivamente formam a empresa. É importante estender o entendimento da organização interna de forma genérica e aplicável a quaisquer outras empresas.

É importante salientar, que cada empresa define, baseada em seu ramo de atuação, quais as prioridades em termos de hardware e software são necessárias, ou ainda, essenciais para melhoria da produtividade, buscando sempre o melhor custo/beneficio para a corporação. O setor de TIC não só têm que responder às necessidades empresariais recentemente percebidas, mas, com a mudança das tecnologias, têm que adaptar procedimentos e práticas. Adequar a capacidade de processamento e armazenamento ao porte da empresa de forma que atenda a necessidades em relação à carga e ao fluxo de informações das transações eletrônicas.

3.1 Gestão de Recursos de Hardware e Software

3.1.1 Critérios gerais

Os usuários devem garantir o controle de acesso às estações de trabalho sob sua responsabilidade. Evitando o uso indevido e acessos não autorizados às informações da empresa. As sessões de trabalho devem ser encerradas ao fim do expediente, ou quando o usuário se ausentar de sua estação de trabalho por períodos prolongados de tempo, desligando ou bloqueando seu equipamento no período de ausência.

A unidade gestora dos recursos de informática, pode monitorar e restringir o acesso aos recursos de informática, através de políticas de segurança implementadas por software ou hardware, monitorando e impedindo alterações nos componentes de software ou hardware. Visando a implementação destas políticas, as estações de trabalho cliente, devem utilizar como padrão o sistema operacional homologado e licenciado pela empresa, observando que o equipamento atenda os requisitos mínimos de hardware.

Em quaisquer ambientes informatizados, sejam corporativos ou não, o uso de senha é um aspecto fundamental da segurança da informação, pois é a primeira barreira para proteção das contas de acesso dos usuários contra pessoas não autorizadas. A senha deve ser individualizada e secreta. O uso de uma senha de má qualidade, ou seja, senha que possa ser

revelada com facilidade, dependendo dos níveis de acesso do usuário, pode resultar no comprometimento de todo o ambiente informatizado da corporação. “O processamento e armazenamento de informações devem ser desenvolvidos respeitando os elementos de controle interno da política de segurança da informação.” (CUNHA, 2006)

Conforme Constituição Federal, Artigo 5º, Inciso XXII e XXIII, a empresa pode se reservar o direito de acesso, auditoria, revisão, eliminação, revelação ou uso de todas as informações armazenadas nos microcomputadores, inclusive verificação de correio eletrônico da Companhia a qualquer momento e sem notificação prévia, ou seja, verificar logs (registros) para análise de acessos impróprios e tomar as devidas providências para evitar o uso indevido. O objetivo é dar maior segurança às informações da empresa.

3.1.2 Gestão de software

A unidade de serviços de TIC deve ficar responsável pelo provimento, homologação, licenciamento, desenvolvimento, suporte e manutenção do software necessário ao provimento dos subsídios tecnológicos para as funções administrativas, operacionais, financeiras, entre outras existentes no âmbito da Companhia.

A SANEPAR possui normas que orientam os usuários sobre a correta utilização dos computadores e software instalados. Ainda existe rígido controle de utilização de internet, e-mail, software de mensagens instantâneas e aplicativos do sistema corporativo. O controle é feito através de autenticação no servidor com login e senha individual. Nos locais onde os computadores são logados a rede através de autenticação no servidor de domínio, o usuário é responsável pela correta utilização do computador a partir do momento que realiza seu login na rede corporativa. O servidor de domínio permite gerenciar de forma individualizada a utilização dos computadores. Porém, nas cidades do interior do estado os computadores não são logadas ao servidor de domínio por causa da baixa banda de comunicação existente no momento e que inviabiliza o procedimento. Mesmo

assim, todos os acessos à internet e a qualquer aplicativo corporativo são feitos sob a exigência de login e senha. E ainda, o conteúdo da internet é filtrado utilizando servidor proxy com serviço Squid e servidor NAT. Existem listas de acesso que permitem ou bloqueiam o conteúdo solicitado. O software antivírus também é uma importante ferramenta utilizada para inibir problemas de vírus, invasões e outras pragas virtuais.

> No ambiente corporativo, software antivírus e de gerenciamento de rede, por questões de segurança, não podem ser desabilitados ou impedidos de funcionar, ficando o responsável sujeito à advertência. (CUNHA, 2006)

A utilização de correio eletrônico (e-mail), é outro recurso que precisa ser muito bem administrado, deve ser feita por usuários autorizados, com a finalidade de agilizar os contatos de negócio, sendo proibido o uso para envio de mensagens que não sejam de interesse da empresa ou que possam comprometer a imagem da empresa perante seus clientes e a comunidade em geral.

Em cada setor da empresa, os ativos (sistemas, aplicações e diretórios) utilizados no ambiente informatizado devem possuir gestores responsáveis por gerenciar a utilização correta, garantindo a aplicação dos níveis adequados de confidencialidade, integridade e disponibilidade nas informações, dados e processos envolvidos. Gerenciar o controle de acesso, autorizando as solicitações de acesso dos usuários e definindo o nível de acesso (somente leitura ou leitura e escrita).

Nessa linha de aplicação, são necessários soluções de software que auxiliem as equipes de TIC. Por exemplo, ferramentas de TI para o gerenciamento de redes. Como é o conceito de administração zero implementável no Windows 2000 Server. Segundo ORTIZ (2001, pág.105), “a administração zero é um conjunto de procedimentos que tenta reduzir o custo total de posse das redes de computador. Quanto maior a rede, mais custos ela gera para a empresa”.

O Active Directory é outra ferramenta importante para a gestão da rede corporativa. Com ele, cada usuário precisa

estar cadastrado no servidor para conseguir logar em qualquer estação de trabalho da empresa.

> O Active Directory é um banco de dados de contas, que é compatível com diversas soluções de protocolos abertos, entre eles estão o LDAP, o DNS e o KERBEROS. Um banco de dados de contas nada mais é que um banco de dados que armazena informações sobre todos os recursos disponíveis na rede (ORTIZ, 2001, pág.197).

Outro exemplo interessante, em termos de ferramentas de TI para o gerenciamento de rede corporativa e que está sendo utilizado pela Companhia de Saneamento do Paraná é a suíte Trauma Zero (Tz0). É um conjunto de módulos de software voltados para a administração de recursos de informática, possibilitando a centralização das informações, permitindo maior segurança e controle para a empresa. Através de uma coleta detalhada dos dados, disponibiliza informações precisas sobre utilização e licenciamento de software, inventário completo de software e hardware, falhas de segurança, entre outras que permitem um melhor uso e maior segurança dos recursos da empresa, racionalizando e otimizando sua utilização. Possibilita o suporte e a manutenção remota, assim como o monitoramento de todas as estações de trabalho mesmo em conexões lentas, criação de políticas de uso das estações e controle do hardware e software instalado.

A suíte Trauma Zero é utilizada da seguinte forma: o software agente é instalado através de *login script* e fica rodando em cada computador da rede. Durante a carga do sistema operacional o agente se conecta ao servidor. O gerenciamento é feito através da Console do Trauma Zero que fica restrito aos administradores da rede. A ferramenta permite o completo monitoramento dos recursos de hardware e software remotamente e a geração de relatórios estatísticos e gerencias eficazes para tomadas de decisão.

Esta solução atende as seguintes necessidades da empresa:

- Gestão do parque de máquinas instaladas na rede corporativa;

- Gestão de hardware instalado nas estações;
- Gestão de software instalado;
- Suporte remoto às estações clientes;
- Melhor utilização dos recursos das estações.

Os recursos apresentados são exemplos de casos de uso. Cada empresa precisa fazer um estudo detalhado das suas necessidades, para a aquisição das soluções que melhor atendam ao perfil da empresa.

3.1.3 Gestão de Hardware

A gestão de hardware diz respeito à padronização do parque tecnológico da empresa. A aquisição ou substituição de equipamentos em série ou lotes, permite uma melhor padronização de hardware *desktop* da empresa. A instalação, configuração e manutenção de hardware tornam-se mais fáceis com a utilização de clonagem de disco rígido. Este procedimento funciona através da utilização de software, que cria uma imagem matriz a partir de um computador instalado e configurado. Essa imagem pode ser replicada para ilimitado número de equipamentos que possuem as mesmas características de hardware, sem problema algum. A outra vantagem é que essa mesma imagem pode ser salva e retornada quando o computador apresentar problemas de funcionamento causados por software.

A Companhia de Saneamento do Paraná adota uma padronização para configuração de computadores bastante interessante. Os discos rígidos são particionados em unidade C (Sistema), onde fica armazenado o sistema operacional e uma partição estendida - unidade lógica D (Dados), onde ficam armazenados os dados do usuário, como pasta Meus Documentos, pasta *Desktop*, pasta Favoritos, pasta Dados de Aplicativos, uma pasta de E-mail e uma pasta Suporte que contém software necessário para reinstalações futuras, *drivers* de configuração e a imagem matriz. Dessa forma o suporte técnico consegue minimizar o tempo de manutenção e recuperação dos computadores. Esta configuração é feita para todos os computadores *desktop* da rede corporativa.

Numa empresa corporativa a atualização ou substituição de hardware deve acompanhar a evolução das necessidades exigidas pelo software utilizado, e também, deve ser dimensionada de forma adequada para a utilização dos usuários, procurando distribuir os equipamentos com maior capacidade de processamento para as áreas que mais necessitam, como por exemplo, área de projetos e engenharia e direcionando os computadores com menor capacidade para áreas de menor exigência de processamento, como por exemplo, atividades administrativas simples. Isso minimiza a sub-utilização e aumenta o período de tempo de utilização do hardware dos computadores na empresa.

4. CONCLUSÕES

As empresas corporativas necessitam de padronização para gestão do parque tecnológico de hardware e software. Isso fica evidenciado na necessidade de existência de um departamento de informática eficaz e competente, que estabeleça critérios e procedimentos normativos, buscando padronizar a aquisição, utilização, suporte e manutenção, tanto de hardware quanto de software, como forma de minimizar os problemas de heterogeneidade e outras incompatibilidades, que podem gerar custos e dor de cabeça a gerência de TIC da empresa. Os investimentos em tecnologia precisam estar muito bem embasado em parâmetros técnicos para que sejam realizados de forma acertada, proporcionando melhorias à empresa, e não se tornando um gasto desnecessário.

Conforme declara GRAEML

> O destino de uma organização pode ser afetado profundamente por suas decisões tecnológicas. A ousadia nessas horas pode levar a casos de sucesso de grande repercussão ou a estrondosos fracassos. (GRAEML, 2000)

Da forma como foi visto, a padronização e o uso inteligente dos recursos tecnológicos podem se não impedir, mas com certeza, minimizar em muito os problemas com tecnologia da informação, promovendo uma maior interoperabilidade dos

recursos corporativos. Da mesma forma que, é extremamente importante estabelecer diretivas e procedimentos de segurança, que garantam a integridade das informações de relevância armazenadas em microcomputadores, bem como o gerenciamento do fator humano, que se apresenta como um dos principais ativos na gestão e manipulação de informações que devem ser trabalhadas, respeitando os elementos de controle interno da política de segurança e informações da empresa.

Observados os fatores apresentados, os objetivos de maximizar a segurança das informações corporativas, podem ser alcançados, sem cair em armadilhas que se apresentam no setor de TIC.

5. REFERÊNCIAS

CUNHA, N.M. **Uso do Ambiente Informatizado**. Companhia de Saneamento do Paraná. PF/INF/001-10, Curitiba, 2006. p.1-5.

GERENCIAMENTO de Infra-estrutura. Disponível em: <http://www.criterium.com.br/site/content/home/template-foto-acima.asp?secao_id=54>. Acesso em: 03 ago. 2006.

GRAEML, A. R. **Sistemas de Informação: o alinhamento da estratégia de TI com a estratégia corporativa.** São Paulo: Atlas, 2000.

ORTIZ, E. B. **Microsoft Windows 2000 Server**. Instalação, Configuração e Implementação, 5. ed. Érica. São Paulo. 2001. Pág. 105, 197.

REZENDE, P. A. D. **Responsabilidades e Escolhas num mundo de Chaves Públicas**, Brasília, 11 Jun. 2003. 60p. Universidade de Brasília. Disponível em: http://www.iti.br/twiki/pub/Forum/ArtigoA04/a04-rezende.rtf. Acesso em: 03 ago. 2006.