Universidade Católica de Brasília

Pró-Reitoria de Pós-Graduação e Pesquisa

Coordenação de Pós-Graduação em Latu Sensu em Informática

MBA em Gestão de Sistemas de Informação

Segurança da Informação na Universidade "X"

André Luiz

Luiz Mauro Pucci

Rossana Rios

Thiers Carlos

Professor: Ly Freitas

Brasília, DF – Brasil

Junho de 2003

Segurança da Informação na Universidade "X" [1]

André Luiz[2]
Luiz Mauro Pucci
Rossana Rios
Thiers Carlos

Resumo

A informação é um bem de valor muito elevado para as instituições fazendo dos métodos utilizados para sua preservação trabalhos dos mais exigentes e valorizados pelos que a administram. Tal relevância necessita ser enfocada em todos os aspectos: humanos, tecnológicos, operacionais e organizacionais tendo na Tecnologia da Informação (T.I.) o estabelecimento da estrutura necessária para prover o Sistema de Informação (S.I.). Esta tecnologia é o meio através do qual toda a instituição pode acessar a informação com a segurança necessária, possibilitando o processamento e armazenamento da mesma com confiabilidade, integridade, confidencialidade e disponibilidade mantendo-a passível de averiguações legais ou técnicas.

Palavras-chave

Informação; Bem; Instituição; Sistemas de Informação (S.I); Métodos; Tecnologia da Informação (T.I); Confiabilidade; Integridade; Confidencialidade; Disponibilidade; Averiguações.

Information's Security of the University "X"

Summary

Information is a very high value good for the institutions, making the methods used for its preservation, the most demanding and appreciated by the ones which administrate it. Such relevance needs to be focused in all aspects: humans, technological, operational, organizational having in Information's Technology the establishment of the necessary structure to cater the System of Information. This technology is the way trough the one every institution can access the information with the necessary security, enabling the processing and storing of the same with reliability, integrity, confidence and availability, keeping it earthly of legal or technical investigations.

Keywords

Information; Goods, Institution; Information's Systems (I.S.); Methods; Information's Technology (I.T.); Reliability; Integrity; Confidence; Availability; Investigations.

[1]Trabalho desenvolvido como parte da disciplina Segurança da Informação do MBA em Gestão de Sistemas da Informação da UCB, no 1º semestre de 2003

[2] Todos os autores são alunos do curso MBA em Gestão de Sistemas da Informação da UCB

1. Introdução

Conhecer a maneira através da qual uma instituição lida com a sua informação é com certeza uma maneira de conhecer essa instituição. E as condições de segurança nas quais essa informação se encontra inserida são premissas da preservação e disponibilização da mesma. Esta necessidade tem se tornado uma prática cada vez mais comum e muitas vezes imperceptível à primeira vista, mas mesmo sem saber que estão fazendo isso os executivos têm a sua maneira de tomar tais providências.
No caso de uma universidade este universo é bastante abrangente por ser a informação que trafega através de seus sistemas de importância relevante para os que dela se utilizam visando o aprimoramento dos seus conhecimentos, e até dos conhecimentos da comunidade. Vale lembrar que além do corpo docente e discente há também os funcionários da área administrativa, que apesar de não lidarem com informações de pesquisa, que é a principal atividade da instituição, lidam com todos os sistemas de controle da instituição e que também necessitam de atenção. É necessário porém que todos os esforços possíveis sejam direcionados aos métodos que possam permitir que essa informação esteja pronta a ser acessada no momento que estas pessoas necessitam dela, assim como que ela seja uma informação correta. E a este pacote de procedimentos que podem propiciar tais condições chamamos de segurança da informação. É o meio que os gestores têm de fazer valer a importância desse patrimônio e eles têm feito isto através de recursos tecnológicos, humanos e organizacionais.

2. Justificativa

A universidade "X" é uma instituição que possui as características citadas e cujo controle não atende às necessidades de preservação da informação. Se faz necessário um estudo dos ativos informacionais visando a identificação da situação na qual se encontra para se conhecer a melhor opção de solução da mesma. Pela relevância da informação para a instituição se faz premente o estabelecimento de uma Política de Segurança da Informação assim como a utilização de Tecnologias da Informação visando uma solução permitindo melhor utilização da mesma. Para isto se faz necessário a realização de entrevistas e aplicação de questionários a funcionários, usuários e estudantes assim como auditoria em sistemas, processos e procedimentos e vistoria de instalações.

3. Objetivo

Com a análise do caso percebe-se o nível de criticidade da situação envolvendo riscos, vulnerabilidades e dentro deste contexto estabelece-se o que precisa ser feito avaliada a relação custo x benefício. Neste caso é necessário a identificação do problema, a solução que pode ser sugerida e o que se espera com a solução proposta. Este enfoque faz-se em vários aspectos, desde a estrutura organizacional, passando pelo trabalho de conscientização dos funcionários, a utilização de hardwares e softwares, o pessoal, o ambiente físico até os procedimentos. Todo esse enfoque está voltado para a necessidade já identificada inicialmente de se estabelecer Política de Segurança para permitir melhorias como confiabilidade, disponibilidade, integridade, confidencialidade

e averiguações de processos e dados através de auditorias. Sendo o resultado do trabalho a que este estudo se propõe uma oportunidade de estabelecer tais recursos.

4. Estudo de caso (situação atual)

O levantamento da situação atual da Universidade "X" tornou-se possível através de inventário de materiais e recursos humanos ligados aos ativos informacionais, assim como uma avaliação das instalações físicas. Com isto os aspectos sugeridos foram analisados e a situação atual foi identificada.

4.1 – Estrutura Organizacional

O estudo de caso revelou uma estrutura organizacional na qual o Departamento de Processamento de Dados se encontra subordinado ao Departamento da Área de Exatas como mostra a Figura 1.

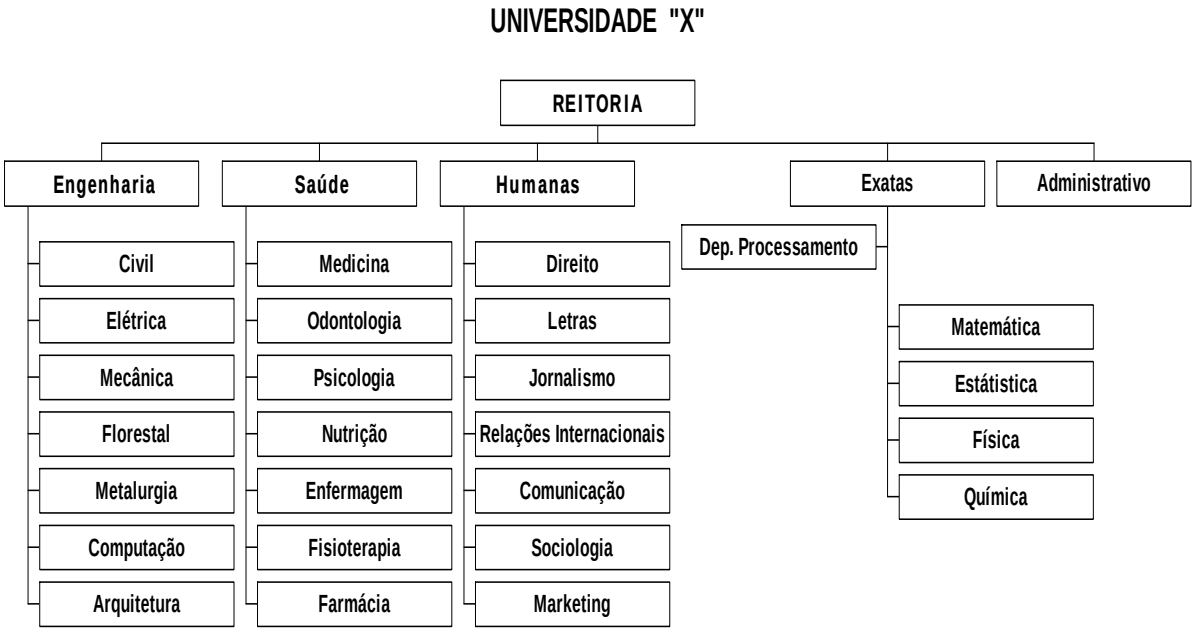

Figura 1 – Estrutura Organizacional da Universidade "X"

Cada departamento possui dotação orçamentária própria podendo investir seus recursos em diversos projetos, inclusive aquisição de hardware, software ou a ampliação de sua capacidade instalada. O departamento de Processamento de Dados tem como funções a administração do Mainframe e das bases de dados coorporativas, a interconexão dos equipamentos à rede e a gestão de segurança.

4.2 - Hardware

A universidade possui um parque de equipamentos instalados composto por:

1 Mainframe
10 Servidores (4 Risc e 6 Intel)
2.000 estações de trabalho (PC´s, Mac´s)
40 Notebooks
200 Impressoras

Todos os equipamentos estão interligados em rede, exceto os notebooks. Os equipamentos estão distribuídos pelos diversos departamentos que se comunicam entre si ou com o Mainframe. Existem servidores que estão no limite de sua capacidade e os elementos de rede não possuem padronização. As redes lógicas também não estão padronizadas. A falta de padronização também se encontra nas estações tanto no que se refere aos fabricantes quanto às características técnicas. A grande maioria dos equipamentos está fora de garantia sendo dada manutenção corretiva por empresa terceirizada.

4.3 - Software

Por se tratar de um centro acadêmico e de pesquisa a Universidade "X" possui um grande número de softwares específicos a cada departamento. Dentre os softwares básicos utilizados citamos:

Sistemas Operacionais	Banco de Dados	Segurança
• Windows 2000 Server	• DB2	• Firewall
• Windows NT Server	• SQL Server	• VirusScan
• Windows NT Workstation	• Oracle	• Norton Antivirus
• Windows 98	• Sybase	
• Linux		
• SunOS		
• HP-UX		
• MacOS		

Figura 2 – Softwares básicos utilizados na Universidade "X"

Os softwares são adquiridos pelas unidades e não possuem nenhum controle centralizado quanto ao número de série, versão e suporte do fornecedor.

4.4 – Pessoal

O pessoal não possui capacitação adequada e é insuficiente, assim como sua distribuição nas equipes e nos turnos de trabalho não atende à demanda. Havendo

concentração de funções nas mãos de poucos funcionários sem a documentação das atividades e procedimentos realizados. O pessoal com acesso aos servidores não possuem identificação. Não são também preparados para combater incêndios e nem lidar com situações inesperadas.

4.5 – Ambiente Físico

Os prédios onde se encontram os equipamentos possuem instalação elétrica inadequada ou sub-dimensionada. Os servidores na sua grande maioria não estão protegidos por geradores e/ou nobreaks, não pertencendo ao circuito essencial. Do qual está fora também o sistema de refrigeração. Na sala dos servidores o controle de acesso está danificado o que caracteriza a não funcionalidade do mesmo. A rede de telefonia é subdimensionada inclusive a que se conecta ao servidor de internet. E os equipamentos de combate a incêndio são insuficientes com extintores vencidos ou inadequados ao local. Além disso o piso falso é desnivelado.

4.6 – Procedimentos

Existem poucos procedimentos operacionais documentados a ponto de se considerá-los inexistentes. Os procedimentos de auditoria não foram identificados como confiáveis nem adequados. A realização de backup´s não tem periodicidade na execução e a documentação é desatualizada. A manutenção dos servidores e estações é do tipo corretiva provocando muitas paradas nos serviços. A instalação e a utilização de softwares se dá sem o devido registro e controle.

5. Problemas Detectados

Os problemas encontrados a partir da situação identificada no estudo de caso foram apontados como de maior ou menor grau de criticidade que deverão ser abordados de acordo com a prioridade estabelecida. O plano de segurança também deverá ser implantado atendendo a este critério. A detecção dos problemas também obedecerá aos aspectos considerados no estudo de caso.

5.1 – Estrutura Organizacional

O Departamento de Processamento de Dados na condição de subordinado ao Departamento da Área de Exatas demonstra que possui pouco ou nenhum poder. E este fato dificulta e até impede que as políticas estabelecidas para T.I., que é de responsabilidade deste departamento, sejam seguidas e/ou obedecidas por todos.

5.2 – Hardware

Os servidores estão descentralizados o que impede o estabelecimento de uma política que garanta a disponibilidade de recursos, através da distribuição de serviços. Além de impedir a distribuição balanceada da carga desses equipamentos. A não padronização dos elementos de rede causa conflitos com interrupção parcial de serviços e a dificuldade na identificação e/ou resolução dos problemas pela transferência desses elementos entre os fornecedores. Os equipamentos também não são padronizados o que exige um estoque elevado de peças, aumentando os custos da manutenção, grande número de fornecedores e prestadores de serviços de manutenção, assim como lentidão no processo de recuperação uma vez que equipamentos distintos exigem instalações diferentes.

5.3 – Software

A ausência de inventário permite a instalação de cópias não legalizadas impedindo o conhecimento das reais necessidades existentes, implicando em gastos desnecessários. A falta da política de atualização de versões gera incompatibilidade entre os aplicativos e obriga à aquisição do mesmo aplicativo para cada uma das versões existentes.

5.4 – Pessoal

Com o levantamento de pessoal foi identificado a sobrecarga de trabalho, gerando vários problemas entre eles a falta de cumprimento de prazos, extrapolação da jornada de trabalho com excesso de pagamento de horas extras. Outro ponto foi o conhecimento de determinados serviços restrito a poucos funcionários tornando a Instituição refém do funcionário. Assim como a ausência de identificação funcional que traz graves problemas de segurança, possibilitando a entrada de pessoas estranhas às áreas restritas da Instituição.

5.5 – Ambiente Físico

Foi identificado com o estudo risco de incêndio causado por sobrecarga elétrica dos quadros de energia, constatado pelas medições efetuadas. E por causa de equipamentos de combate a incêndio ausentes, inadequados ou vencidos. A ausência de circuito elétrico essencial através de nobreaks e/ou geradores foi identificada também como causador de problemas no ambiente físico como queda dos servidores sem o devido processo de baixa danificando alguns equipamentos, corrupção de base de dados e refrigeração inadequada de equipamentos. O acesso indevido à áreas de acesso considerado restrito também caracterizou um problema uma vez que não existe controle para esses acessos na Instituição. O servidor de internet ligado a uma rede de telefonia subdimensionada mostrou também que dificulta e até impede a conexão de novos

usuários tornando lento o acesso dos já existentes. Além dos riscos de acidentes causados pelo desnivelamento do piso falso.

5.6 - Procedimentos

Procedimentos operacionais não documentados causam erros operacionais, não divulgação do conhecimento (o conhecimento fica restrito aos poucos funcionários que executam determinada tarefa) e impedimento de avaliação e melhoria de processos. Outro problema encontrado foi a má qualidade dos backup´s realizados com ausência de periodicidade, documentação adequada e de testes de recuperação de backup´s.
As interrupções de serviços têm sido causadas pela inexistência de manutenções periódicas. A falta de controle e registro de softwares tem ocasionado a contaminação por vírus. Prejuízos financeiros também são sentidos uma vez que a falta de licença para utilização de um software gera multa e processos judiciais. Além disso não é possível uma identificação adequada dos problemas ocorridos devido aos processos de auditoria existentes serem insuficientes ou inadequados.

5.7 – Ameaças

Dentro desta fase do estudo foi identificado um outro aspecto além dos já citados: as ameaças. Estas são perdas, roubos ou vandalismos causados aos ativos informacionais pela ausência de controle de acesso, de procedimentos operacionais, de inventário de software e instalação indiscriminada destes causando inclusive problemas judiciais e financeiros. Outra ameaça é a sobrecarga de energia elétrica provocando corrupção, indisponibilidade e comprometendo a integridade dos dados.

5.8 – Vulnerabilidade

A vulnerabilidade é mais um aspecto além dos já conhecidos e mostra justamente como a instituição fica com seu ambiente e informação vulneráveis, isto devido à ausência de controle de acesso, insuficiência de treinamento de pessoal inclusive de combate a incêndio, pessoal com sobrecarga de trabalho, falta de procedimentos operacionais no tratamento das informações, instalação indiscriminada de softwares, ausência de equipamentos de incêndio ou inadequação dos mesmos.

5.9 - Análise de Risco

A análise de risco mostra na verdade o risco que a instituição possui, isto baseado nas vulnerabilidades e ameaças que esta apresenta. Sendo assim tanto maior será o risco calculado quanto maiores forem as vulnerabilidades e ameaças. E o nível do risco será então proporcional ao risco calculado, valor do ativo e as consequências que este risco traz à Instituição.

6. Proposta de Solução

A proposta de solução baseia-se no levantamento da situação atual e problemas detectados procurando desta forma sugerir uma solução que possa ser mais adequada às condições da Instituição, levando em consideração que não se tem intenção de sugerir aumento de gastos ou aquisição de novos equipamentos, a não ser aqueles que realmente forem necessários. Um outro enfoque a ser considerado é a questão da adoção ou não da proposta que fica a cargo da Instituição, assim como a consideração por parte desta em questionar quaisquer dos itens sugeridos como solução. A proposta de solução também faz referência aos aspectos considerados nas etapas anteriores.

6.1 – Estrutura Organizacional

Com a identificação do problema que o Departamento de Processamento de Dados não tinha poder de decisão a sugestão de solução é a alteração na estrutura organizacional colocando o Departamento de Processamento de Dados na condição de staff de reitoria como mostra a figura 3.

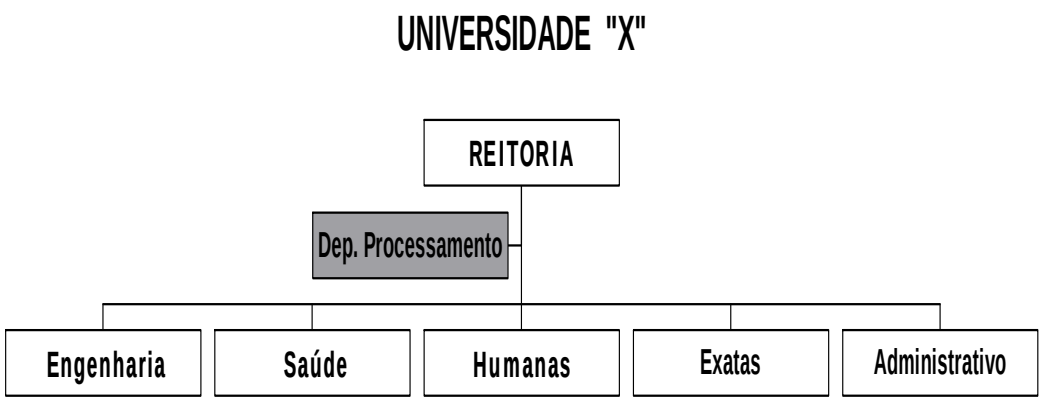

Figura 3 – Sugestão de Estrutura Organizacional da Universidade "X"

6.2 - Hardware

Para os hardwares diante da situação encontrada e dos problemas identificados a proposta de solução sugere a centralização dos servidores para permitir replicação e uma melhor distribuição dos serviços e otimização do balanceamento da carga operacional. A padronização das máquinas e dos elementos de rede visando um menor estoque de peças de reposição, menor custo de manutenção, menor número de fornecedores e/ou prestadores de serviço de manutenção e possibilitando agilização nas reinstalações.

6.3 – Software

No caso dos softwares a proposta é que seja realizado um planejamento de atualizações de softwares. Um inventário dos já existentes identificando as reais necessidades nesta área, inclusive com a instalação de um software específico para inventariamento automático de softwares e hardwares. Assim como a proibição da instalação de softwares por pessoal não autorizado.

6.4 – Pessoal

No que se refere a pessoal notou-se que a readequação de pessoal pela centralização de serviços é uma proposta de solução adequada à questão da sobrecarga de trabalho, assim como excesso de horas extras e má distribuição das tarefas.
A necessidade de treinamento de pessoal é outro ponto importante visto que permite a preparação dos funcionários para lidar com situações adversas, inclusive de acidentes com incêndio.
A identificação obrigatória também se faz necessária dentro deste contexto uma vez que teria todos os funcionários devidamente identificados, principalmente aqueles que têm acesso às áreas de acesso restrito.

6.5 – Ambiente Físico

No ambiente físico o redimensionamento da rede elétrica visando suportar a demanda é uma proposta de solução para o caso das sobrecargas identificadas como problemas. A utilização de nobreaks e/ou geradores também se faz necessária uma vez que evitaria a queda repentina da rede impedindo que os dados sejam corrompidos ou apagados. Outro redimensionamento necessário é o dos equipamentos de refrigeração assim como sua conexão ao circuito essencial possibilitando um ambiente adequado às máquinas.
Quanto ao controle de acesso aos ambientes restritos a proposta de solução é o uso de equipamentos biométricos visando maior segurança no acesso.
Revisão e adequação dos equipamentos de combate a incêndio e o estabelecimento de uma política de manutenção dos mesmos visando evitar riscos pela falta ou inadequação destes.
Substituição da rede telefônica do servidor de internet por um canal de maior banda e velocidade visando capacitar a rede a atender seus usuários.

6.6 – Procedimentos

A falta de documentação identificou problemas quanto aos procedimentos o que sugere uma proposta de documentação dos procedimentos operacionais com a normatização do seu uso. Os backup´s também exigem o estabelecimento de um cronograma assim como a automatização do processo objetivando maior produtividade,

qualidade e confiabilidade. Incluída nesta proposta está a implementação de testes periódicos de recuperação de backup´s.
Outro aspecto importante é a manutenção de equipamentos e elementos de rede através do estabelecimento de um programa de manutenção preventiva evitando paradas repentinas nos sistemas e indisponibilidade de acesso.
A necessidade de estabelecer procedimentos e normatização para instalação e homologação de novos softwares e aplicativos possibilita uma melhor utilização dos mesmos.

6.7 – Contingência, Auditoria, Confidencialidade, Integridade e Disponibilidade

6.7.1 - Contingência

Diante das ameaças verificadas na detecção de problemas mais um aspecto passa a ser considerado na proposta de solução que é a contingência, ou seja, a utilização de meios para garantir que ameaças não deixem a informação indisponível.
A utilização de máquinas espelhos para serem utilizadas no caso de parada repentina dos servidores.
Ter máquinas substitutas sempre disponíveis para casos de quebras.
Manter backup´s diários em outras instalações, empresas.

6.7.2 – Auditoria

A auditoria é outro aspecto identificado com os problemas, uma vez que praticamente não existia.
Em relação aos bancos de dados os serviços são registrados em log´s que permitem, identificar o usuário que solicitou o serviço, em qual máquina, data e horário sendo possível rastrear o que o usuário fez.
Quanto aos softwares a proposta é o controle das licenças e dos softwares instalados.
Já com relação aos hardwares o controle é sugerido através do número patrimonial.

6.7.3 – Confidencialidade

Este é mais um aspecto identificado com os problemas mostrando que a informação ficava exposta a acessos tanto por rede quanto por ambiente físico pela falta de controle nos mesmos.
A proposta é um controle de pessoas através de senhas individuais e intransferíveis de acesso visando maior confidencialidade aos serviços.
Uma outra parte da proposta para senhas de acesso é a criptografia de senhas de acesso ao banco de dados.

6.7.4 – Integridade

A falta de integridade também foi identificada pela falta de controle de acesso à rede e aos ambientes físicos, tendo também como proposta de solução que a autorização para alteração e/ou exclusão de dados seja dada através de senhas apenas a pessoas que sejam responsáveis pelas informações.
A disponibilização dos backup´s das alterações.

6.7.5 – Disponibilidade

A disponibilidade é um aspecto muito importante uma vez que impacta o acesso aos sistemas. Pelo que foi observado na detecção de problemas quanto a esse aspecto a proposta é a utilização de geradores automáticos visando que o sistema não pare em caso de queda de energia possibilitando assim o acesso à informação.
A redundância nos serviços críticos é outra proposta no intuito de permitir disponibilidade da informação, visando a continuidade dos serviços em caso de sobrecarga de solicitações (BD, internet, etc...).

7. Resultados Esperados

Depois da proposta de solução baseada nos problemas detectados no estudo de caso vem a fase dos resultados esperados com a sugestão dada. Mais uma vez estes resultados são esperados seguindo os mesmos aspectos considerados nas etapas anteriores. Com isto tem-se condições de avaliar o levantamento que foi feito.

7.1 – Estrutura Organizacional

Com a alteração na estrutura organizacional sugerida na proposta de solução espera-se que o Departamento de Processamento de Dados tenha uma redefinição nas suas atribuições e papéis podendo assim fazer respeitar as políticas de segurança da informação através da função de normatização.

7.2 – Hardware

Pela proposta de centralização espera-se uma melhor distribuição de serviços. Com a padronização dos equipamentos espera-se a redução do estoque de peças de manutenção, redução do custo das manutenções, redução do número de fornecedores e/ou prestadores de serviço de manutenção assim como uma maior agilização na própria manutenção que era lenta e difícil.

7.3 – Software

Uma maior confiabilidade dos serviços espera-se com a proposta de controle das atualizações de softwares. Espera-se a criação de um catálogo para controle e dimensionamento das reais necessidades com a proposta de inventariamento dos softwares e aplicativos. Um outro controle que se espera é o de acesso às instalações permitindo confiabilidade e integridade dos sistemas e das bases de dados.
Um outro ponto da proposta é o planejamento das atualizações que espera-se permitir ganho de escala para aquisição de novos produtos, redução de custos através de softwares instalados, maior integridade nas aplicações dos sistemas, maior disponibilidade do sistema pela compatibilização e pela redução nas interrupções.

7.4 – Pessoal

Em relação a proposta sugerida ao pessoal o que se espera com a readequação do pessoal é uma melhor distribuição das atividades, melhor aproveitamento do quadro de funcionários, redução de custos com pessoal e cumprimento de prazos de entrega de serviços. Através do treinamento das equipes espera-se ganhos de produtividade e qualidade assim como estímulo através do aprimoramento pessoal.

7.5 – Ambiente Físico

De acordo com a proposta para o ambiente físico espera-se atender adequadamente a demanda, reduzir riscos de incêndio e de acidentes, aumentar a confiabilidade e a disponibilidade com o redimensionamento da rede elétrica.
Com a utilização de nobreak´s e/ou geradores espera-se evitar quedas repentinas da rede e a corrupção de dados mantendo a integridade da base.
O controle de acesso por meio de equipamentos biométricos espera uma identificação segura dos funcionários autorizados e ganho de confidencialidade.
Com a revisão e adequação de equipamentos de combate a incêndio juntamente com o estabelecimento de uma política de manutenção espera-se um aumento do nível de segurança das instalações e do pessoal bem como ganho de confidencialidade.
No tocante à rede de telefonia com a sua substituição espera-se maior velocidade nas conexões e no tráfego de informações, um maior número de conexões e um suporte maior para novas tecnologias.

7.6 – Procedimentos

O que a proposta aponta como solução para os procedimentos é a documentação dos procedimentos operacionais, permitindo com isso a disseminação do conhecimento operacional.
Quanto aos backup´s a proposta de melhoria no processo espera reduzir o volume de informação perdido por incidente e um aumento da produtividade, qualidade e confiabilidade.

Na proposta de solução foi mostrada a necessidade de implementação de teste de recuperação de backup visando integridade e confiabilidade.
Outra proposta foi o estabelecimento de manutenção preventiva reduzindo as interrupções para manutenções corretivas assim como seus custos.
Em relação à proposta de estabelecer procedimentos de instalação e homologação de softwares espera-se com sua aplicação redução da possibilidade de contaminação por vírus, eliminação de problemas judiciais pelo uso ilegal de software e maior confiabilidade do sistema.

8. Conclusão

Segurança da Informação é um dos assuntos mais discutidos e um dos recursos mais solicitados pelas organizações na atualidade. O que talvez não seja tão atual é a maneira como isto vem sendo feito no decorrer do tempo, pois mesmo os mais antigos comerciantes já se preocupavam em manter sua informação de forma segura, não utilizando os recursos dos executivos de hoje mas com certeza com artifícios que eram suficientes na época que usavam. Mas o que talvez seja mais interessante em todo este contexto de segurança da informação é o quão abrangente ele se faz. De acordo com o levantamento que foi feito no caso objeto deste estudo todas as áreas da organização estão inseridas na questão da segurança da informação, desde a estrutura da organização até o ambiente físico, o pessoal e os procedimentos. Isto leva a reflexão da necessidade de se estabelecer trabalhos periódicos para avaliação de todo o processo considerado no estabelecimento da política de segurança da informação. Mesmo depois da implantação desta política é necessário que no decorrer de um período (um ano ou dois) esta política seja revista pois mudanças no mercado principalmente no tocante às tecnologias alteram processos ou comportamentos que podem comprometer a manutenção da política. Inclusive e principalmente a questão da conscientização por parte dos integrantes da organização, desde a mais alta gerência executiva ao mais simples funcionário. Porque se em alguma parte da organização esta consciência se dispersa ou deixa de ser cumprida pode representar um abalo na condução dos serviços e até que isto seja detectado é provável que danos sérios possam ter sido causados. Por isso tão importante quanto o estabelecimento e a implantação de uma política de segurança da informação em uma organização é a manutenção e preservação da mesma, e um passo importante para facilitar este trabalho é a questão da conscientização por parte de todos.
Deste modo é fácil perceber que o trabalho para se identificar, propor, estabelecer e implantar uma política de segurança da informação não é fácil visto que depende de vários aspectos e enfoques diferenciados, mesmo porque o ramo de atividade da organização é fator determinante do tipo de trabalho a ser feito, porém a consciência dos envolvidos em colocar em prática o que se pretende deve ser a motivação maior de todo o trabalho.

9. Referências Bibliográficas

[DIAS CLÁUDIA, 2000] DIAS, CLÁUDIA. – *"Segurança e auditoria da Tecnologia da Informação"*. Axcel Books do Brasil Editora, Rio de Janeiro, 218p.

[GIL, ANTONIO DE LOREIRO, 1998] GIL, ANTONIO DE LOREIRO – *"Segurança em Informática"*. Atlas, São Paulo.

[MOREIRA, NILTON S, 2001] MOREIRA,NILTON S – *"Segurança Mínima – Uma Visão Corporativa da Segurança de Informação"*. Axcel Books, Rio de Janeiro.

URL http://www.modulo.com.br