

FARN

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

UM ESTUDO DAS PRINCIPAIS SOLUÇÕES ADOTADAS PELA DISTRIBUIDORA
INTERNACIONAL DE ALIMENTOS PARA GARANTIR A SEGURANÇA DA
INFORMAÇÃO

João Ubirajara Lima dos Santos

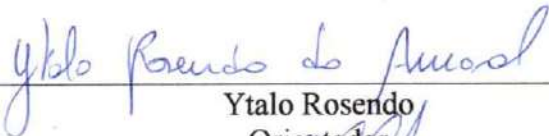
NATAL/2004

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

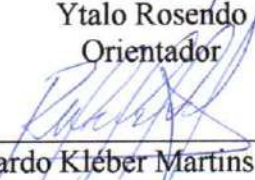
UM ESTUDO DAS PRINCIPAIS SOLUÇÕES ADOTADAS PELA DISTRIBUIDORA
INTERNACIONAL DE ALIMENTOS PARA GARANTIR A SEGURANÇA DA
INFORMAÇÃO

João Ubirajara Lima dos Santos

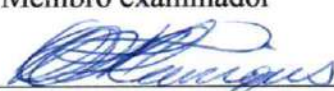
Monografia apresentada e aprovada em 11 de DEZEMBRO de 2004, pela banca de
qualificação composta pelos seguintes membros:



Ytalo Rosendo
Orientador



Ricardo Kléber Martins Galvão
Membro examinador



Pádua Henrique
Membro examinador

Natal, 11 de DEZEMBRO de 2004.



JOÃO UBIRAJARA LIMA DOS SANTOS

UM ESTUDO DAS PRINCIPAIS SOLUÇÕES ADOTADAS PELA DISTRIBUIDORA INTERNACIONAL DE ALIMENTOS PARA GARANTIR A SEGURANÇA DA INFORMAÇÃO

Monografia apresentada ao curso de
Bacharelado em Sistemas de Informação da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do Norte
como requisito parcial para a obtenção do
título de Bacharel em Sistemas de
Informação.

Orientador:
Ytalo Rosendo, MsC.

NATAL/RN

UM ESTUDO DAS PRINCIPAIS SOLUÇÕES ADOTADAS PELA DISTRIBUIDORA
INTERNACIONAL DE ALIMENTOS PARA GARANTIR A SEGURANÇA DA
INFORMAÇÃO

Monografia, apresentada ao curso de
Bacharelado em Sistemas de Informação da
Faculdade Natalense para o
desenvolvimento do Rio Grande do Norte
como requisito parcial para a obtenção do
título de Bacharel em Sistemas de
Informação.

Catálogo na Publicação – Biblioteca da FARN identificação

Setor de Processos Técnicos.

Santos, João Ubirajara Lima dos

Um estudo das principais soluções adotadas pela Distribuidora Internacional de Alimentos para garantir a segurança da informação. /João Ubirajara lima dos santos. _____ Natal: FARN, 2004. 41p.

Orientador: Ytalo Rosendo do Amaral(MsC)

Monografia (Graduação em sistemas de informação) – Faculdade Natalense para o desenvolvimento do Rio Grande do Norte.

1. Tecnologia da Informação – Monografia I. Título

SUMÁRIO

1. INTRODUÇÃO.....	7
1. OBJETIVOS.....	8
1.1 OBJETIVO GERAL.....	8
1.3 OBJETIVOS ESPECÍFICOS.....	8
1.3 JUSTIFICATIVA.....	8
2. REFERENCIAL TEÓRICO.....	9
2.1 INFORMAÇÃO.....	9
2.2 CLASSIFICAÇÃO DA INFORMAÇÃO.....	9
2.3 ATIVO DA INFORMAÇÃO.....	10
2.3.1 EXEMPLOS DE ATIVO.....	11
2.4 SEGURANÇA DA INFORMAÇÃO.....	11
2.5 OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO.....	11
2.6 ANÁLISE DE RISCOS.....	13
2.7 AMEAÇAS.....	14
2.8 VULNERABILIDADES.....	15
2.9 CONTROLES.....	16
2.10 POLÍTICA DA SEGURANÇA DA INFORMAÇÃO.....	16
2.11 TECNOLOGIAS DE APOIO A SEGURANÇA DA INFORMACAO.....	18
2.11.1 FIREWALL.....	18
2.11.1.2 TIPOS DE FIREWALL.....	18
2.11.2 IDS.....	19
2.11.3 VPN.....	19
2.11.4 CRIPTOGRAFIA.....	20
2.11.5 PLANO DE CONTINGENCIA.....	21
2.11.6 BACKUP.....	21
2.11.7 ENGENHARIA SOCIAL.....	21
2.11.8 PRAGAS VIRTUAIS.....	22
2.11.9 HACKERS.....	23
3. METODOLOGIA.....	24
4. ANÁLISE DOS RESULTADOS.....	25
5. CONCLUSÃO.....	35
6. REFERÊNCIAS BIBLIOGRAFICA.....	38

RESUMO

Esta monografia apresenta um estudo feito sobre as ferramentas adotadas pela DIA – Distribuidora Internacional de Alimentos Ltda, para garantir disponibilidade, integridade e confidencialidade da informação gerada dentro do ambiente corporativo. Para isso, foi desenvolvido um estudo junto com a equipe de informática, um estudo que além de mapear as ferramentas usadas no ambiente, identificou algumas possíveis vulnerabilidades e suas soluções. Primeiramente, são descritos os conceitos de alguns tópicos abordados no trabalho como informação, segurança da informação, plano de contingência e ameaças. A principal ênfase do trabalho foi dada à observação dos recursos e artifícios utilizados pela empresa para garantir a integridade, disponibilidade e confidencialidade da informação. Finalizando, são propostas algumas melhorias que tem como objetivo contribuir com o trabalho já realizado pela empresa.

Palavras-chave

Integridade

Disponibilidade

Segurança

Informação

ameaça

ABSTRACT

This work presents a study of the tools used at DIA – Distribuidora Internacional de Alimentos Ltda, to guarantee availability, integrity and confidentiality of the information that is created into the corporative environment. For this, we developed a study with the IT team that identified the used tools in the environment and some possible vulnerabilities. First, we showed some concepts like information, security, security of the information, firewall, plan of contingency, threats and viruses. The main emphasis of the work was given to the comment of the resources and artifices used for the company to guarantee the information. Finishing, we proposed some solution that could contribute with the security of the information of the company.

Key-words

Integrity

Availability

Information

Security

1 INTRODUÇÃO

A Segurança da Informação tem sido um dos temas mais discutidos na área de TI (tecnologia da informação). Também existe uma preocupação de como os departamentos de informática das empresas estão tratando o assunto, assim a segurança da informação e a forma pela qual ela é tratada vêm sendo estudadas já há algum tempo. Podemos dizer que a revolução pela qual estamos passando está contribuindo bastante com toda essa atenção dada a segurança da informação, pois sabemos que essa nova era, a chamada era do conhecimento, na qual o bem mais precioso será produzido pela junção do pensamento de vários indivíduos, os quais o usaram como diferencial competitivo seja qual for o propósito. Esse bem ao qual nos referimos é a Informação.

Se por um lado podemos fazer uso deste “novo bem” para melhorarmos nossas vidas, por outro, esse mesmo bem pode ser usado contra nós. Assim, devemos dar um tratamento muito especial à informação, procurando protegê-la de qualquer tipo de ameaça que venha a colocar em risco sua integridade, disponibilidade e confidencialidade.

A fragilidade das empresas no que diz respeito à segurança da informação vem tirando o sono de muitos empresários, técnicos e especialistas da área de tecnologia da informação, uma vez que a quantidade de material produzido e os ataques a eles realizados vêm aumentando de forma exponencial. Vários fatores devem ser levados em consideração quando falamos de como se deve gerenciar a informação produzida no ambiente corporativo.

O tipo de conhecimento hoje exigido dos profissionais da área de TI vai muito além do que saber fazer uma atualização de um servidor ou mesmo identificar um ataque contra sua rede. Esse tipo de conhecimento é importante, porém questões como crimes digitais, e-mail como prova judicial e monitoramento de usuários dentre outras coisas, devem ser de conhecimento desses profissionais, mais precisamente do *Security Officer*, que é como se chama o responsável pela segurança da informação no ambiente corporativo.

Assim, acreditamos ser de extrema importância sabermos como os departamentos de tecnologia da informação estão tratando a segurança da informação dentro dos seus ambientes, como os profissionais desses setores estão se atualizando e o que é mais importante, descobrimos qual é o nível de interação que o alto escalão da empresa tem com o setor de TI quando o assunto é segurança da informação.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

O objetivo geral deste projeto é tentar mapear dentro de uma empresa do mercado local, como a empresa vem tratando a segurança da informação, procurando identificar o uso de ferramentas que possam contribuir com a manutenção da segurança da informação.

1.2.2 Objetivos Específicos

Contribuir para a melhoria dos processos através da identificação de possíveis falhas, e dar sugestões que possam ajudar na eliminação das falhas identificadas.

1.3 JUSTIFICATIVA

Quando pensamos em informação, estamos pensando em algo íntegro, confiável e que nos ajudará a resolver algum tipo de problema. Da mesma forma são as corporações que fazem uso da informação para se destacar no mercado do qual elas fazem parte. Só que para garantir que a informação vai estar sempre íntegra, confiável e disponível, é de extrema importância que ela seja mantida por uma equipe que conheça o valor que a informação possui para a organização. Quando esse trabalho não é feito de forma correta os prejuízos podem ser tão grandes a ponto de abalar qualquer empresa independente de seu tamanho, tempo de mercado ou área de atuação.

Por fazer parte de uma área relativamente nova, a segurança da informação apesar de ser bastante desafiadora e de grande interesse para os profissionais de tecnologia, ainda não é considerado de alta prioridade para a maioria das empresas. Essa obra pretende dar uma orientação básica os profissionais da área de TI sobre alguns pontos que devem ser analisados quando se fala em segurança da informação. Tal proposta tem o objetivo de ser útil às empresas e profissionais que estiverem começando a levantar informação sobre segurança da informação.

2. REFERENCIAL TEÓRICO

Para um melhor entendimento desta obra, serão apresentados alguns conceitos de grade importância para o desenvolvimento do estudo ao qual o trabalho se propõe.

2.1 INFORMAÇÃO

A preocupação com proteção da Informação não é algo que surgiu recentemente. Podemos identificar em varias fases da trajetória humana a preocupação com a segurança de algo que, para a época, seria ou teria o mesmo valor que a informação tem nos tempos atuais.

A informação é um ativo de muito valor para toda e qualquer organização, pois na maioria dos casos, pode influenciar diretamente no negócio da empresa, sendo então de grane importância protegê-la da melhor forma possível. Para realizar esse trabalho de proteção da informação, usamos a segurança da informação, que visa proteger a informação contra ameaças diversas, procurando minimizar o risco e, procurando aumentar a continuidade dos negócios, além de procurar maximizar o retorno dos investimentos (NBR ISSO/IEC 17799, 2001).

2.2 CLASSIFICAÇÃO DA INFORMAÇÃO

Nem toda informação deve ser protegida e, algumas, devem ser altamente protegidas. Para que se possa realizar um bom trabalho, no que diz respeito à proteção da informação, é essencial que se possa levantar qual informação possui a necessidade de ser protegida.

A classificação da informação pode se dar da seguinte forma:

- Pública – informação que não possui valor suficiente, de tal forma que se for a público não afetará os negócios da organização;
- Interna pública – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
- Interna – o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso desautorizado não sejam por demais serias. Sua integridade é importante, porquanto não seja vital;
- Confidencial – Informação restrita aos limites da empresa, cuja divulgação ou perda pode levar ao desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente, além de permitir vantagem expressiva ao concorrente;

- **Secreta** – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital à companhia.

Não é difícil perceber que a informação é algo extremamente importante para toda e qualquer empresa, uma vez que o acesso e a utilização da informação de forma correta, podem garantir um diferencial competitivo à empresa que a possua. Assim, a informação passa a ter um papel cada vez mais importante dentro do ambiente corporativo, fazendo com que as empresas tenham que dar uma maior atenção à informação e fazer investimentos cada vez maiores para protegê-la. Dessa necessidade surgiu a Segurança da Informação.

2.3 - ATIVO DE INFORMAÇÃO

Os ativos da informação são formados por três elementos, que são, as informações, os objetos que as suportam e as pessoas que as utilizam. Um ativo é todo elemento que compõe o processo de comunicação, a contar da informação, seu emissor, o meio pelo qual ela trafega e o seu receptor. Os ativos são os elementos que a segurança da informação visa proteger. Eles possuem um valor para a empresa e em consequência, precisam ter uma proteção adequada para que os negócios não sejam prejudicados (MÓDULO SECURITY, 2003).

CASTRO FILHO (2003), define ativos de informação como sendo todas as informações disponíveis dentro da organização na forma de banco de dados e documentos, e que são relevantes para o negócio da empresa. Exemplos de ativos de informação são listas de fornecedores, indicadores financeiros, estrutura de material de produtos, características técnicas dos seus produtos, informações dos seus clientes, propostas comerciais e etc. Essas informações, se perdidas, acessadas ou alteradas indevidamente, podem gerar problemas de qualidade ou interrupções nos serviços, e como consequência a perda de produtividade.

2.3.1 Exemplos de Ativo (MÓDULO SECURITY, 2003).

Equipamentos: estes ativos representam toda a infra-estrutura tecnológica que suporta a informação durante seu uso, tráfego e armazenamento. Os ativos pertencentes a esse grupo são os computadores, os servidores, notebooks, mídias, equipamentos de conectividade, ou seja, elementos de uma rede onde as informações trafegam e são armazenadas.

Aplicações: este grupo de ativos contém todos os programas de computador utilizados na automatização de processos. Dentre eles citamos os softwares de mercado, programas institucionais, sistemas operacionais, etc. A segurança da informação busca avaliar a forma

como as aplicações são criadas, como estão disponibilizadas e como são utilizadas pelos usuários e por outros sistemas.

Informação: este grupo de ativos engloba os elementos que contêm a informação registrada, em meio magnético ou físico, como documentos, relatórios, livros, manuais, correspondências patentes, contracheques de funcionários planos estratégicos de mercado, e etc.

Usuários: este grupo refere-se aos indivíduos que fazem uso dos recursos de comunicação da empresa e que manipulam as informações. O foco da segurança da informação nos usuários está voltada à conscientização de ou para formação de hábitos para a tomada de decisão, e da ação por parte de todos os funcionários de uma empresa que vai desde a alta direção até os usuários finais.

Organização: neste grupo, estão os itens que compõem a estrutura física e organizacional da empresa. Quanto ao ambiente físico, são considerados salas e armários onde estão armazenados os documentos, fitas, salas de servidores e etc.

2.5 - SEGURANÇA DA INFORMAÇÃO

“Segurança de informação é, portanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança”.(DIAS 2002)

A NBR ISO/IEC 17799 (2001), coloca que para se atingir os objetivos da segurança da informação, é necessário o uso de uma série de ferramentas de controles tais como políticas, procedimentos e práticas. Além disso, o uso de recursos de softwares e hardware, estruturas adequadas, pessoas capacitadas, apoio de empresas especializadas, são indispensáveis quando se espera ter bons resultados no que diz respeito à segurança da informação.

2.6 - OBJETIVOS DA SEGURANÇA DA INFORMAÇÃO

A expectativa de todo usuário, no que diz respeito à segurança de dados, é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo. Essas expectativas podem ser traduzidas em objetivos de segurança.

Uma vez que a segurança da informação pode ser implantada de forma a ter objetivos diferentes dependendo do ambiente ao qual se está procurando proteger, não seria possível classificar todos os objetivos de segurança da informação.

Segue alguns dos principais objetivos de segurança (DIAS, 2000):

Confidencialidade ou privacidade - proteger as informações contra acesso de qualquer pessoa não explicitamente autorizada pelo dono da informação, isto é, as informações e os processos são liberados apenas para pessoas com autorização previa.

Integridade de dados - evitar que dados sejam apagados ou de alguma forma alterados, sem a permissão do proprietário da informação. O conceito de dados nesse objetivo é mais amplo, englobando dados, programas, documentação, registros, fitas magnéticas e etc. O conceito de integridade está relacionado com o fato de assegurar que os dados não foram modificados por pessoas não autorizadas.

Disponibilidade - proteger os serviços de informática de tal forma que não sejam degradados ou tornados indisponíveis sem a devida autorização. Para um usuário autorizado, um sistema não disponível, quando se necessita dele, pode ser tão ruim quanto um sistema inexistente ou destruído.

Consistência - certifica-se de que o sistema atua de acordo com as expectativas dos usuários autorizados. Se um software ou hardware passa a se comportar de maneira totalmente diferente da usual, normalmente após alterações de hardware ou software, isso pode causar dados irreparáveis.

Isolamento ou uso legítimo - regular o acesso ao sistema. O acesso não autorizado é sempre um problema, pois além de ser necessário identificar quem acessou e como, é preciso se certificar de que nada importante do sistema foi adulterado ou apagado. As medidas corretivas após uma invasão podem envolver tempo e recursos financeiros consideráveis para análise do sistema e sua reconstrução ou recuperação, se for o caso.

Auditoria - proteger os sistemas contra erros e atos maliciosos cometidos por usuários autorizados. Para identificar os autores e suas ações, são utilizadas trilhas de auditoria e logs, que registram tudo que foi executado no sistema, por quem e quando. Em algumas aplicações críticas, as trilhas de auditoria podem incluir operações de restauração ao estado inicial, auxiliando o trabalho de reconstrução do sistema original.

Confiabilidade - garantir que, mesmo em condições adversas, o sistema atuará conforme esperado.

Antes de se pensar em proteger alguma coisa, é de extrema importância que se mapeie o que deve ser protegido e qual a importância que o ativo (informação) mapeado tem para os negócios da organização.

O SECURITY HANDBOOK (2001) que foi publicado pela SYMANTEC, diz que as organizações devem identificar os dados e sistemas que são essências para o seu sucesso. Esses elementos possuem além de valores monetários, valores são que intrínsecos.

As organizações devem se perguntar quais os ativos de informação são críticos para os seus negócios, e quais os danos causados caso um desses ativos venha a se tornar indisponível. Perguntas do tipo:

Qual o impacto para o nosso negócio se essa informação que consideramos essenciais estiver indisponível para nos por que foi roubada, perdida, corrompida ou propositalmente apagada?

Qual o impacto para o nosso negócio se essa informação crítica não puder ser utilizados por um determinado período de tempo?

Quando custaria para a organização se, por exemplo, uma ferramenta de trabalho como o correio eletrônico estivesse inacessível por um dia ?

Quanto perderia a organização se os consumidores não pudessem entrar em contato por que a página da organização está temporariamente indisponível?

Além desses questionamentos, as organizações devem se perguntar como ficaria a sua credibilidade e reputação perante o mercado, pois determinada ameaça não causa apenas prejuízo financeiro, causa também prejuízo à imagem da organização.

Quando temos respostas às essas e outras perguntas, temos material suficiente para passarmos para o passo seguinte que é a análise de riscos.

2.7 - ANÁLISE DE RISCO

A análise de risco é um dos pontos mais críticos no processo de segurança da informação. É nesse estágio, que serão levantadas as informações importantes para serem utilizadas nas definições dos controles e recurso que precisaremos para garantir que os objetivos da segurança da informação sejam alcançados.

Segundo a NBR ISSO/EIC 17799 (2001), quando se faz uma avaliação sistemática dos riscos de segurança, podemos identificar os requisitos de segurança.

A Análise de risco pode ser dividida em cinco partes de igual importância, porém, quando analisadas de forma isolada, estas partes representam muito pouco ou quase nada. Alinhados e geridos de forma adequada, estes componentes de análise de risco apontaram caminhos seguros na busca do nível adequado de segurança de uma organização. Os cinco pontos são:

- Identificação e classificação dos processos do negócio;
- Identificação e classificação dos ativos;
- Análise de ameaças e danos;

- Análise de vulnerabilidades.

SÊMOLA (2003), acrescenta:

Executar uma verdadeira análise de riscos é transcender os aspectos puramente tecnológicos e realizar o mapeamento dos seus processos de negócio, seus planos estratégicos e seus valores. É identificar as características físicas, tecnológicas e humanas que suportam e mantêm a empresa ativa. É estar orientado por uma metodologia de análise subsidiada por uma base de conhecimento viva, munido de ferramentas e profissionais voltados a diagnosticar as ameaças e os riscos que efetivamente oferecem perigo à continuidade operacional. É oferecer como resultado um diagnóstico guiado pelo negócio e para o negócio, coerente com os anseios dos executivos, com um plano de ação priorizado para os gestores e informações operacionais para os técnicos.

Uma análise de riscos deve ser realizada sempre antecedendo um investimento. Antes de a organização iniciar um projeto, um novo processo de negócio, o desenvolvimento de uma ferramenta ou até mesmo uma relação de parceria, deve-se mapear, identificar e assegurar os requisitos do negócio. O processo de análise de riscos deve envolver especialistas em análise de riscos e especialistas no negócio da empresa — esta sinergia possibilita o foco e a qualidade do projeto. Um projeto de análise de risco sem o envolvimento da equipe da empresa, muito dificilmente retratará a real situação da operação. A execução do projeto deve ser realizada em tempo mínimo. Em ambientes dinâmicos a tecnologia muda muito rapidamente. Um projeto com mais de um mês — em determinados ambientes —, ao final, pode estar desatualizado e não corresponder ao estado atual da organização. Conhecer o risco é ganhar mobilidade. Alguns riscos — como o choque de um avião contra o nosso prédio —, só poderão ser evitados a um alto custo; não é isso que queremos. Esse diagnóstico, que até bem pouco tempo ocultava-se sobre pequenas e isoladas iniciativas do grupo de tecnologia da informação, quase sempre relacionado a aspectos técnicos da famosa “análise de vulnerabilidades tecnológicas”, já é reconhecido como ferramenta de suporte estratégico (RAMOS, 2002).

2.8 AMEAÇAS

As ameaças são agentes capazes de explorar falhas de segurança, que se chama de vulnerabilidades e, conseqüentemente, causa perdas ou danos aos ativos de uma empresa, trazendo impacto ao seu negócio. Os ativos são constantemente submetidos a ameaças que podem colocar em risco a integridade, confidencialidade e disponibilidade das informações. Estas ameaças sempre existiram, pois também estão relacionadas a causas naturais, internas

ou externas que venham a representar risco para a empresa. No entanto, a segurança da informação visa implantar formas de controle que impeçam a concretização dessas ameaças, garantindo que o negócio da empresa não seja prejudicado. As ameaças são constantes e podem ocorrer a qualquer momento. As ameaças podem ser divididas em três grandes grupos, que são eles: Naturais, Intencionais e Involuntárias. Antes decidir como proteger um sistema, é necessário saber contra que ele será protegido. A segurança pode, então, ser definida em termos de combate às ameaças identificadas. A análise das ameaças e vulnerabilidades do ambiente de informática, deve levar em consideração todos os eventos adversos que podem explorar as fragilidades de segurança desse ambiente e acarretar danos. É claro que o custo de se proteger contra uma ameaça pode ser mais alto do que o dano que essa ameaça pode provocar, isto é, nem todas as ameaças merecem ser combatidas. É necessário fazer uma análise de custo benefício antes de tomar qualquer medida (DIAS, 2000).

2.8.1 VULNERABILIDADE

As vulnerabilidades são os elementos que uma vez explorados por ameaças, afetam a integridade, confidencialidade e disponibilidade das informações de um indivíduo ou empresa. As vulnerabilidades são os elementos que devem ser rastreados e eliminados do ambiente de tecnologia, sendo este um dos primeiros passos para implantação de um ambiente seguro. (MÓDULO SECURITY, 2003).

A MÓDULO SECURITY (2003) divide as vulnerabilidades nas seguintes categorias:

Físicas: São aquelas de ordem física, presentes nos ambientes em que a informação é armazenada ou manipulada.

Naturais: São aquelas relacionadas às condições da natureza que possam colocar em risco as informações.

Hardware: Muitas são os elementos que representam vulnerabilidades de hardware. Dentre elas podemos citar a falta de atualização dos programas que são orientados pelo fabricante ou a conservação inadequada dos equipamentos.

Software: os softwares são os elementos que fazem à leitura das informações e que permitem aos usuários acessarem as mesmas.

Mídias: As mídias são os suportes físicos ou magnéticos utilizados para armazenar informação. Dentre eles estão os disquetes, cd-roms, fitas magnéticas, discos rígidos de servidores, estorages, assim como o arsenal documentário registrado em papel.

Comunicação: Este tipo de vulnerabilidade abrange todo o tráfego da informação. Onde quer que a informação trafegue, seja via cabo, satélite, fibra ótica ou ondas de radio, deve haver segurança.

Humanas: Esta categoria de vulnerabilidade esta relacionada aos danos que as pessoas podem causar as informações e ao ambiente tecnológica que as suporta.

2.9 CONTROLES

Uma vez que os riscos e vulnerabilidades foram identificados e o impacto foi calculado, devemos identificar quais controles deveram ser usados. A norma NBR ISSO/EIC 17799 (2001) sugere vários controles, porem, existe casos que não são possíveis aplicarmos um determinado controle. Já em outros casos, há a necessidade de se criar controles que não são contemplados pela norma.

NBR ISSO/EIC 17799 (2001) enumera uma serie de controles que são considerados essências para uma organização, sob o ponto de vista legal.

- a) Proteção de dados e privacidade de informações essências;
- b) salvaguarda de registros organizacionais;
- c) direitos de propriedade intelectual;
- d) relatório dos incidentes de segurança;
- e) gestão da continuidade do negocio.

Como já mencionada acima, a norma não contempla todos os controles. Assim, deve-se procurar na norma os controles que são aplicáveis à organização e criar os controles que não encontramos na norma.

Uma vez identificados os controles, deve-se criar estratégias que nos permita controlar da melhor forma possível esse ambiente vulnerável.

2.10 POLITICA DE SEGURANÇA DA INFORMAÇÃO

A ISO/IEC 17799 (2001) define o objetivo da política de segurança da informação, como sendo o de prover a direção uma orientação e apoio a segurança da informação.

Podemos dizer que a política e um mecanismo que tem como objetivo orientar a empresa na proteção da informação e de todos os processos que são importantes para o bom funcionamento dos negócios.

Uma política é um conjunto de diretrizes, normas e procedimentos e instruções de trabalho que estabelecem os critérios a serem adotados em nível local ou institucional,

visando o estabelecimento, padronização e normalização da segurança junto tanto no âmbito humano quanto tecnológico. A partir dos seus princípios, é possível tornar a segurança da informação um esforço comum, visto que todos poderão contar com um arsenal informativo documentado e normalizado, voltado à padronização do *modus operandi* de cada um dos indivíduos envolvido na gestão da segurança da informação. A política é elaborada tendo-se por base a cultura da organização e o *know-how* de segurança dos profissionais envolvidos com a sua aplicação e comprometimento. É importante considerar que para elaboração de uma política de segurança, seja formada uma equipa multidisciplinar que represente grade parte dos aspectos culturais e técnicos da organização e que se reúne periodicamente, dentro de um cronograma estabelecido pelo Comitê de Segurança. Esse comitê é formado por um grupo definido de pessoas responsáveis por atividades referentes à criação e aprovação de novas regras de segurança na organização. Nas reuniões são definidos os critérios adotados em cada área e o esforço comum necessário para que a segurança atinja um nível mais alto. Deve-se ter em mente que as equipes envolvidas devem ter tempo livre para analisar e escrever todas as regras discutidas nas reuniões. A oficialização de uma política tem por base a aprovação da administração da organização. A política deve ser pública e comunicada de forma adequada a todos os empregados, parceiros, terceiros e clientes se necessário (MÓDULO SECURITY 2003).

Nesse documento devem estar expressas as preocupações da administração da organização, onde são estabelecidas regras para a gestão da segurança da informação, contendo: a definição da própria política, uma declaração da administração apoiando os princípios estabelecidos e uma explicação dos requisitos de conformidade quanto a:

- Legislação e cláusulas contratuais;
- Educação e treinamento em segurança da informação;
- Prevenção contra ameaças (vírus, trojans, hackers, incêndios, intempéries, etc.).
- Princípios, objetivos e requisitos necessários para a operação da empresa e para o processamento da informação.

Deve conter também a distribuição das responsabilidades das pessoas envolvidas, onde estejam claros os papéis de cada um na gestão dos processos de segurança.

Não devemos esquecer de que toda documentação já existente sobre a condução das tarefas deve ser analisada quanto aos princípios da segurança da informação, aproveitando ao máximo as práticas correntes, avaliando e agregando segurança a essas tarefas (MÓDULO SECURITY, 2003)

2.11 TECNOLOGIAS DE APOIO A SEGURANÇA DA INFORMAÇÃO

Existe uma necessidade muito grande por tecnologias que ajudem no combate as ameaças capazes de impedir que os objetivos da segurança da informação sejam atingidos. Para um melhor entendimento, vamos analisar de forma superficial algumas dessas tecnologias.

2.11.1 Firewall (HAZARI, 2000).

Firewall são ferramentas baseados em hardware ou software que tem como objetivo cuidar do tráfego não desejado ou não autorizado que tenha como origem uma rede promiscua, tal como a Internet. Assim a tecnologia de firewall permite que os usuários internos possam acessar recursos externos a rede local e que os serviços que estão na rede interna possam ser acessados por usuários externos, sem causar dano à empresa (FREIRE, 2002)

Assim, sua principal função é a análise do tráfego entre a rede interna e externa, bloqueando o tráfego de acordo com regras pré-definidas.

2.11.1.2 Tipos de Firewall (HAZARI, 2000).

- Filtragem de pacotes

O firewall que trabalha na filtragem de pacotes é muito utilizado em redes pequenas ou de porte médio. Por meio de um conjunto de regras estabelecidas, esse tipo de firewall determina que endereços IPs e dados podem estabelecer comunicação e/ou transmitir/receber dados. Alguns sistemas ou serviços podem ser liberados completamente, enquanto outros são bloqueados por padrão, por terem riscos elevados. O grande problema desse tipo de firewall, é que as regras aplicadas podem ser muito complexas e causar perda de desempenho da rede ou não serem eficazes o suficiente.

- Firewall de aplicação

Firewalls de controle de aplicação são instalados geralmente em computadores servidores e são conhecidos como proxy. Este tipo não permite comunicação direto entre a rede e a Internet. Tudo deve passar pelo firewall, que atua como um intermediador. O proxy efetua a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Este tipo de firewall é mais complexo, porém muito seguro, pois todas as aplicações precisam de um proxy. Caso não haja, a aplicação simplesmente não funciona. Em casos assim, uma solução é criar um "proxy genérico", através de uma configuração que informa que determinadas aplicações usarão certas portas. Essa tarefa só é bem realizada por administradores de rede ou profissionais de comunicação qualificados.

2.11.2 IDS

IDS quer dizer Sistema de Detecção de Intrusos (Intrusion Detection System/Firewall), que é a arte de detectar atividades estranhas na rede de computadores. Sistemas de IDS que operam em um host com o objetivo de detectar atividades suspeitas são chamados de IDS baseados em host, e os sistemas de IDS que operam de forma a analisar o tráfego da rede são chamados de IDS baseados em rede. (SANS, 2004)

Assim, sua principal função é a análise do tráfego entre a rede interna e externa, bloqueando o tráfego de acordo com regras pré-definidas.

A detecção de intruso pode ser feita de dois modos (SANS, 2004):

- Sensores procuram por "assinaturas" de ataques, que são os métodos utilizados por invasores e catalogados no IDS;
- Sensores detectam alguma atividade suspeita, seja por eventos não esperados ou diferentes do perfil normal de usuário ou aplicação.

Para que se possa realizar o monitoramento de um sistema, um sistema de detecção de intruso deve seguir alguns aspectos básicos (PELISSARI, 2002):

- Funcionamento constante em segundo plano sem interação;
- Base de dados não pode ser perdida em caso de falha do sistema operacional;
- Automonitoração;
- Funcionamento imperceptível no sistema;
- Detecção de alterações do funcionamento normal;
- Difícil de ser enganado;
- Detecção de poucos falsos positivos;
- Não detecção de falsos negativos;
- Não permissão de subversão.

2.11.3 VPN

Rede virtual privada ou do inglês *Virtual Private Network*, é a extensão da rede privada de uma empresa permitindo que pessoas autorizadas possam fazer uso dos recursos

internos como correio eletrônico, acesso a documentos, acesso ao software de gestão dentre outras coisas, de forma segura e confiável. A VPN permite que dados importantes sejam enviados e recebidos a través de redes compartilhadas ou públicas como a Internet (MICROSOFT, 2000).

Existem muitas técnicas que podem ser usadas na implementação de VPN, abaixo são listadas algumas (MICROSOFT, 2000):

Modo Transmissão – somente os dados são criptografados, não havendo mudança no tamanho dos pacotes;

Modo Transporte – somente os dados são criptografados, podendo haver mudança no tamanho dos pacotes;

Modo Túnel Criptografado – os dados e o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e de destino.

Modo Túnel Não Criptografado – tanto os dados quanto o cabeçalho são empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino.

2.11.4 Criptografia

O objetivo da criptografia é deixar a informação ilegível, tornando a mesma incompreensível para qualquer pessoa que não seja o dono ou pessoa por ele autorizada. (OLIVEIRA, 2001).

Criptografia é a ciência (e arte) de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para: autenticar a identidade de usuários, autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias, e proteger a integridade de transferências eletrônicas de fundos (NBSO, 2003)

Criptografia de chave pública e privada - Nesse sistema de criptografia, existe a utilização de duas chaves, uma que deve ser informada livremente e outra que deve estar em poder da pessoa ou instituição. A informação que criptografada com uma determinada chave pública só poderá ser decriptografada com a chave privada correspondente (OLIVEIRA, 2001).

2.11.5 Plano de contingência

Quando temos algum que é vital para o nosso negócio, não podemos contar apenas com o que está em uso, pois caso o perdamos por qualquer motivo, estaremos em apuros.

Um plano de continuidade ou recuperação de desastre a recursos tecnológicos deve ser parte do plano geral de contingência que a empresa possui. O plano de continuidade é constituído por um conjunto de procedimentos que devem ser definidos formalmente para permitir que a empresa possa trabalhar em caso de falha de algum dos seus componentes e dependendo da extensão do problema, a mesma poderá operar mesmo com um certo grau de degradação. DIAS (2002).

Segue as fases do plano de continuidade (DIAS, 2002):

- Atividades preliminares;
- Análise de impacto;
- Análise das diversas alternativas de recuperação;
- Desenvolvimento do plano de contingência;
- Treinamento;
- Teste do plano de contingência;
- Avaliação dos resultados e atualização do plano.

2.11.6 Backup

Há muitas maneiras de perder informações, com, por exemplo, um pico de voltagem ou uma queda de energia, relâmpagos, inundações, furtos e, às vezes, o equipamento simplesmente pode falhar. O backup regular das informações permite que você recupere algumas (ou todas) das suas informações, caso algo ocorra com os originais no seu sistema.

A política de backup deve conter os procedimentos e a infra-estrutura necessária à proteção de todas as informações que de fato tenham alguma importância. A definição de quando deve ser feito o backup, o local onde o mesmo será armazenado e a periodicidade, deve ser feita com a participação da equipe de TI, de um ou mais representantes da diretoria e com a participação de usuários mais críticos.

Outro ponto muito importante na política de backup é o teste das cópias realizadas. Muitas empresas possuem belas rotinas de backup, porém, quando há a necessidade recuperar alguma informação, pode ocorrer o inesperado, a falha (DIAS, 2002).

2.11.8 Pragas virtuais

O vírus de computador é a primeira tentativa para criar vida artificial, porque o vírus tem todas as propriedades de um organismo vivo. Ele propaga-se, vive num ambiente próprio, move-se e etc. O vírus de computador compartilha algumas das características de vírus biológicos. Um vírus de computador passa de computador a computador como um vírus biológico passa de pessoa a pessoa (CSU, 2001).

Os Vírus de computador são misteriosos e agarram nossa atenção. Por um lado, mostram a nossa vulnerabilidade. Um vírus corretamente criado pode ter um efeito surpreendente na Internet mundial. Por outro lado, eles mostram o quão sofisticado e ligados se tornaram os seres humanos.

A seguir é mostrada uma lista de tipos de vírus (www.scua.net):

Vírus de arquivos ou programas - Vírus que normalmente ficam alojados em arquivos com extensões: .COM, .EXE, .DLL, .SYS, .BIN e .BAT. Exemplos de vírus de programa conhecidos são Jerusalém e Cascade;

Vírus de setor de boot - Vírus que ficam armazenados na inicialização do sistema. Exemplos de vírus de setor de boot são: Form, Disk Killer, Michelangelo e Stoned;

Vírus de macro - Vírus que infectam arquivos dos programas Microsoft Office (Word, Excel, PowerPoint e Access);

Vírus Multipartite - Vírus que infectam setores de boot, disquetes e arquivos executáveis.

Stealth - Vírus que utiliza técnicas para ocultar as alterações executadas e enganar o antivírus.

Vírus Polimórficos - Vírus que se auto modificam a cada nova disseminação. De forma que um único vírus pode ter inúmeras formas diferentes.

Spyware - o spyware é programa independente que podem monitorar as atividades do sistema de maneira secreta. Estes podem detectar senhas e outras informações confidenciais e enviá-las para outro computador.

Worm - o worm é um programa que cria cópias de si mesmo - por exemplo, de uma unidade para a outra - ou copiando-se usando e-mail ou outro mecanismo de transporte. O worm pode comprometer a segurança do computador. Ele pode ser recebido na forma de um programa brincalhão ou software do tipo.

4.11.9 Hacker

O termo Hacker é definido pela RFC (*Request for comments*) 2828 como alguma pessoa com um grande interesse e conhecimento em tecnologia em tecnologia, não utilizando eventuais falhas descobertas em benefício próprio. O termo é usado erroneamente especialmente pelas pessoas que não são da área de tecnologia para definir as pessoas que praticam algum tipo de crime virtual. O termo correto para definir esse tipo de pessoa seria cracker ou intruder que também é definido pela mesma RFC como sendo alguém que tenta quebrar a segurança ou ganhar acesso a sistemas de outras pessoas sem ser convidado.

3. METODOLOGIA

Esta pesquisa classifica-se, de acordo com seus objetivos, como uma Pesquisa Descritiva/Exploratória, pois irá descrever quais os recursos que a empresa DIA utiliza para garantir a segurança da informação.

O método de pesquisa do trabalho será histórico comparativo, pois serão levados em consideração trabalhos anteriores tais como pesquisas já realizadas, trabalhos publicados que tenham sido feitos com o mesmo objetivo.

As fontes de pesquisa classificam-se como Pesquisa de Campo, pois a fonte de dados será uma empresa do mercado local, e os procedimentos técnicos classificam este estudo como um Estudo de Caso, pois será feito um levantamento dos recursos utilizados na gerencia, manutenção e proteção das informações produzidas no ambiente corporativo.

Uma vez que o tema do projeto foi escolhido, optamos pela empresa DIA – Distribuidora Internacional de Alimentos, pois se teria como desenvolver o trabalho com facilidade, uma vez que se trabalha na mesma. Assim, junto ao departamento de informática, colhendo informações suficientes para analisar e chegar a uma conclusão.

O trabalho foi realizado o trabalho através entrevistas e da observação do ambiente. Procuramos realizar o trabalho junto aos membros do setor de TI, o que nos permitiu ver qual o grau de entendimento da empresa quando o assunto é tecnologia e principalmente segurança da informação.

4. ANÁLISE DOS RESULTADOS

Quando pensamos em informação, estamos pensando em algo íntegro, confiável e que nos ajudará a resolver algum tipo de problema. Hoje em dia, é fundamental que uma empresa independente de seu porte, possa fazer uso da informação para se destacar no mercado do qual ela faz parte. Só que para garantir que a informação vai estar sempre íntegra, confiável e disponível, é de extrema importância que ela seja mantida por uma equipe que conheça o valor que a informação possui para a organização. Quando esse trabalho não é feito de forma correta os prejuízos podem ser tão grandes a ponto de abalar qualquer empresa independente de seu tamanho, tempo de mercado ou área de atuação.

Por fazer parte de uma área relativamente nova, a segurança de informação ainda não é prioridade para muitas empresas, logo os departamentos de tecnologia da informação não dão à devida atenção que o tema merece, no entanto, é evidente que tal postura não é culpa única e exclusivamente do departamento de TI, pois boa parte dos executivos que controlam as empresas não sabem dar o devido tratamento a esse ativo que é a informação. Essa obra pretende identificar na empresa analisada o uso de mecanismos que possam contribuir com a segurança da informação. Além disso, pretendemos contribuir com algumas orientações para que melhorar as atividades referentes à segurança da informação.

4.1 O AMBIENTE DE ESTUDO

Dentre varias empresas do setor privado que tinha presença no mercado local, foi escolhida uma do ramo de distribuição de alimentos pois a mesma possui uma parque tecnológico consideravelmente grande quando comparado a outras empresas do estado do RN. Vamos fazer uma breve descrição da empresa, no qual iremos mostrar de forma resumida como se da à aplicação da tecnologia da informação dentro da empresa e quais os pontos que a segurança da informação e imprescindível.

A DIA é uma distribuidora de alimentos que há 10 anos vem representando no estado do Rio Grande do Norte e da Paraíba, em presas como a Fabrica Fortaleza, Sadia industria e comercio, Johnson, Nutriday (para os demais estados brasileiros), dentre outras marcas. Hoje, a DIA conta com duas modalidades de vendas, pré-venda e pronta entrega.

Pré-venda: na pré-venda o vendedor sai com um caminhão carregado e vai realizando as visitas e efetuando as vendas. Para agilizar o processo, o vendedor conta com um equipamento de coleta de dados que possui informações do tipo estoque em transito, numero de notas fiscais, tabelas de preço e clientes a visitar. Tais informações são utilizadas no processo de faturamento, pois e através do equipamento que o vendedor entra com o pedido

do cliente e por fim emite a nota fiscal. O vendedor fica com as informações de por um período de uma semana, descarregando os dados quando o mesmo volta para abastecer o caminhão.

Pronta entrega: a operação de pronta entrega é um pouco mais simples, porém, de forma contraditória, o uso de recursos tecnológico é bem mais acentuado. Nesse tipo de atividade o vendedor não leva consigo a mercadoria, ele apenas realiza as visitas e tira os pedidos que, são enviados a empresa para que junto com outros pedidos de pré-venda possam ser entregues. Nessa atividade, a empresa faz uso de um equipamento tipo Palmtop munido de uma modem e um software, permitindo ao vendedor enviar e receber informações quase que em tempo real.

Na retaguarda, o produto que dá suporte à operação é um software de gestão empresarial, Logix. Para que o produto possa ser utilizado, a empresa deve adquirir uma poderosa ferramenta de banco de dados. Algumas ferramentas de software tiveram que ser desenvolvidas para atender às necessidades específicas da empresa.

A DIA possui uma filial que está situada na cidade de João Pessoa – PB. Por questões estratégicas, a empresa optou por centralizar todos os seus sistemas e conseqüentemente as informações. Assim, para prover acesso à filial de João Pessoa, a DIA faz uso de uma ferramenta computacional chamada de servidor de terminal, permitindo que os funcionários da empresa possam acessar os sistemas de forma remota. Além da filial, a empresa possui representantes comerciais que acessam o sistema de forma esporádica. Outra operação que está sendo iniciada é a operação de Broker, na qual uma empresa que já atua no segmento de distribuição passa a distribuir os produtos que são representados pela DIA.

Para fazer acesso à rede mundial de computadores, a DIA possui uma parceria comercial com a Embratel que, além de fornecer acesso à Internet, também fornece acesso aos vendedores de pré-venda que usam o serviço da Embratel para enviar os pedidos e receber informações da empresa.

Outros serviços não menos importantes são oferecidos pela empresa às pessoas que realizam trabalhos administrativos. Podemos citar, como exemplo, o sistema de correio eletrônico, o sistema de comunicação interna, os sistemas de acesso à Internet, os sistemas de acesso a dados bancários dentre outros.

Para manter essa estrutura, a empresa conta com uma equipe formada por quatro pessoas que desenvolvem atividades distintas.

O departamento de segurança da informação é constituído pela própria equipe de informática, e identificamos apenas uma pessoa que dentre outras atividades, dedica algum tempo à segurança da informação.

4.2 ORÇAMENTO EM 2004

O orçamento da área de TI girou em torno de 260.000,00 (duzentos e sessenta mil reais), dos quais 60% foram destinados à segurança da informação.

4.3 INVESTIMENTOS EM 2004

A empresa espera fazer aquisições importantes no ano de 2004. Como foi informado na pesquisa, foram feitos investimento nas áreas de alta disponibilidade, sistemas de suprimento de energia redundantes, sistemas de backup, antivírus e principalmente capacitação técnica.

4.4 PRINCIPAIS OBSTÁCULOS PARA IMPLANTAÇÃO DA SEGURANÇA

O estudo revela que o maior problema encontrado pelo setor de tecnologia para implantação da segurança da informação é a falta de recurso humano, uma vez que a equipe é bastante reduzida e que não se dedica única e exclusivamente a trabalhos relacionados à segurança da informação, a falta de apoio especializados no que diz respeito a empresas que prestem serviços relacionados à segurança da informação, e a conscientização dos usuários, pois os trabalhos realizados acabam sendo atrapalhados por barreiras culturais.

4.5 PRINCIPAIS AMEAÇAS

Os vírus de computador foram apontados com os grandes vilões desse ano para a empresa. Um outro problema que a equipe de tecnologia vem passando é com relação às informações que acabam saindo das empresas nos notebooks, e as fraudes via e-mail também tem sido alvo das preocupações.

4.6 PRINCIPAIS PROBLEMAS DE SEGURANÇA

Segundo a empresa, o principal ponto de invasão é a internet, por onde mais de 99% dos vírus tentam entrar nos computadores da empresa. As tentativas de invasão que são realizados com técnicas de engenharia social usando o e-mail, também foram apontas como outra grande preocupação da equipe.

4.7 IDENTIFICAÇÃO DE ATAQUES

A equipe de informática já identificou atividades que poderiam ser consideradas ataques a empresa, porém, por falta de tempo, a identificação da origem e as intenções do possível atacante não foram descobertas. No caso de um ataque acontecer, além da correção dos problemas, também é dada uma atenção à vulnerabilidade explorada. A providência adotada e, na maioria das vezes, a correção dos problemas.

4.8 MEDIDAS DE SEGURANÇA JÁ IMPLANTADAS

Como o objetivo principal desse trabalho é identificar dentro da empresa o uso de ferramentas que ajudem na manutenção da segurança da informação, procuramos dar uma atenção maior às ferramentas encontradas e como elas vem ajudando a equipe de informática nas atividades diariamente.

4.8.1 Política de segurança

A empresa não possui uma política de segurança formalizada. Mesmo assim, identificamos alguns mecanismos que levam a crer que já existe certa preocupação por parte do setor de tecnologia no que diz respeito à utilização dessa ferramenta. A equipe de informática desenvolveu alguns controles para facilitar o acompanhamento de atividades que são críticas ao negócio da empresa. Além dos controles identificados, a equipe também desenvolveu alguns procedimentos com o objetivo de padronizar algumas tarefas rotineiras. A empresa já possui certificação ISO9000, o que é um ponto positivo, uma vez que existe a cultura do trabalho guiado por normas e procedimentos.

4.8.2 atualização de softwares

Atualizações sempre serão necessários no ambiente computacional dessa forma, quanto maior for o controle das atualizações dos sistemas, menor será a probabilidade de erros acontecerem. A empresa estuda possui algum procedimento e controles para garantir que as atualizações necessárias sejam feitas da melhor forma possível.

4.8.2.1 Antivírus

O sistema de antivírus utilizado pela empresa permite o gerenciamento automático das atualizações nas estações de trabalho e servidores, mesmo assim, existe um controle manual das atualizações que é realizado através do preenchimento de planilhas. Além do controle de atualizações a equipe de informática desenvolveu um procedimento no qual constam

orientações com, por exemplo, como proceder no caso de identificação de atividades virais, ou como proceder no caso do sistema não conseguir eliminar um determinado vírus e quais os períodos de atualização do servidor de antivírus e das estações de trabalho.

4.8.2.2 Sistema operacional

Como mais 90% dos computadores da empresa utilizam Windows da Microsoft, a equipe de informática usa uma ferramenta de gerenciamento de atualizações disponibilizada pela própria Microsoft (www.microsoft.com/sus) que permite que os sistemas operacionais possam ser atualizados automaticamente. Alguns dos benefícios identificados com a adoção dessa solução foram:

- Controle das atualizações nas estações;
- Diminuição do tráfego no link de comunicação;
- Aumento da produtividade do pessoal de suporte;
- Maior produtividade do usuário final;
- Diminuição do número de vulnerabilidades nas estações;

4.8.2.3 Hardware

As atualizações de componentes físicos são tratadas de acordo com a criticidade do equipamento a ser atualizado. No caso de servidores e ativos de rede, as atualizações são realizadas nos finais de semana e sempre seguindo as orientações dos fabricantes. Toda e qualquer atividade que precise ser feita em componentes considerados críticos, deve ser notificada à diretoria da empresa e se for o caso, os prestadores de serviço que dão suporte diretamente ao equipamento também serão convidados a participar da atividade. No caso de estações de trabalho, os usuários devem ser notificados com certa antecedência. A equipe também possui procedimento formalizado para garantir que as atividades realizadas não causem transtornos aos usuários ou perda financeira para a empresa.

4.8.3 Controle dos acessos

O uso de ferramentas para controlar o acesso à informação, pode ajudar bastante a equipe de informática de uma empresa a manter as informações seguras. Tanto o acesso lógico aos sistemas, com o acesso físico a áreas restritas deve ser controlado. Identificamos a utilização de algumas ferramentas do tipo planilhas para registrar os acessos, e câmeras de vídeo para monitorar as atividades realizadas dentro do ambiente.

4.8.3.1 Contas e senhas

As contas e senhas dos funcionários são criadas apenas por uma pessoa, o gerente de informática, o qual só cria uma conta mediante documento formal do responsável direto pelo funcionário. Não identificamos uma política de senhas formalizada, porém, algumas regras são utilizadas na criação de senhas.

- As senhas devem ter no mínimo 7 caracteres;
- É mantido o histórico das últimas 10 senhas utilizadas pelos usuários;
- As senhas devem ser renovadas a cada mês;
- As contas só podem ser utilizadas em horários predeterminados (Se necessário fazer acesso ao sistema fora do horário, o gerente do setor devera informar a necessidade com antecedência).

Identificamos algumas limitações no sistema que controla as contas e senhas dos usuários, impedindo a aplicação de medidas mais rigorosas na criação e manutenção das contas de usuário. Outro ponto que dificulta a vida dos usuários e a quantidade de contas e senhas de devem ser criadas, pelo fato de não existir um sistema de autenticação unificado. As senhas que dão acesso total aos sistemas, as senhas dos ativos de rede e senhas dos servidores, todas sem exceção, são de conhecimento apenas do gerente de informática.

4.8.3.2 Acesso remoto

O acesso remoto feito pela filial, representantes, vendedores e pessoas em trânsito, são feitos através de uma VPN (*Virtual Private Network*), o que garante a segurança dos dados acessados. Outra forma identificada para fazer acesso aos servidores da empresa é a ferramenta Putty que trabalha com o protocolo SSH, bastante utilizada pela equipe nas atividades de suporte. Um problema identificado com relação ao acesso remoto é que não existe o controle do que é trafegado por dentro do túnel da rede virtual, o que pode ser um grande problema, pois se um invasor conseguir acesso a uma máquina remota, ele irá poder gerar qualquer tipo de tráfego como, por exemplo, passar uma ferramenta que tenta descobrir computadores com portas abertas. Só é permitido o acesso remoto ao sistema de gestão da empresa através de um produto de emulação de terminal, o que aumenta ainda mais a segurança dos dados transferidos, uma vez que o tráfego que passa pelo túnel é o gerado apenas pelas teclas digitadas e pelo vídeo.

4.8.3.3 Acesso físico

Todos os equipamentos de informática considerados críticos, estão instalados em sala específica. O acesso à sala dos servidores, como é chamada, só pode ser feito por pessoas autorizadas, caso contrário, a mesma deverá estar acompanhada do gerente de informática ou pessoa por ele autorizada. Os membros da diretoria têm acesso irrestrito à sala de processamento de dados. Não existe um registro de visitantes ao centro de processamento de dados, o que acaba fragilizando o ambiente.

4.8.4 Monitoramento

O monitoramento é algo que deve ser constante no ambiente computacional, pois é através do monitoramento que se pode saber, por exemplo, se uma medida adotada está sendo cumprida, ou se existe tentativa de burlar as regras da empresa, e em alguns casos, é possível prever problemas futuros dentre outras coisas.

4.8.4.1 Logs de eventos

Todos os ativos de rede e servidores possuem os logs ativados. Uma vez que os arquivos de log são analisados, os mesmos são incluídos nas rotinas de backup caso haja a necessidade. Os logs são verificados manualmente o que acaba dificultando o trabalho devido a grande quantidade de logs a serem analisados. Devida a essa grande quantidade de logs e a falta de pessoa dedicada à segurança da informação, a análise dos logs de eventos é feita de forma superficial o que pode ser bastante prejudicial para empresa, pois no caso de um ataque, a equipe de informática poderá levar dias ou até meses para perceber que esta sendo atacada. Identificamos também algumas falhas com relação aos logs gerados como, por exemplo, a falta de uma área de disco própria para os logs, a falta de uma política que determine o tamanho máximo dos logs, o número mínimo de dias que os logs devem ser mantidos, qual a periodicidade de verificação dos logs, dentre outras coisas que poderiam ajudar na manutenção dos logs de eventos gerados pelo sistema.

4.8.4.2 Tráfego de rede

O tráfego de rede da empresa é analisado apenas quanto ao volume, sendo utilizado para isso ferramentas disponíveis nos próprios ativos de rede como, por exemplo, o software de análise que acompanha os switches da família 3300 da 3COM. Como a rede da empresa é segmentada, a análise de tráfego é feita apenas na rede interna devido ao fato dos ativos da rede externa ou DMZ (rede desmilitarizada) não possuírem recursos de gerenciamento, o que

também pode ser bastante perigoso, pois não se sabe o que trafega nesse segmento. Outro problema identificado com relação ao layout da rede que possui apenas dois segmentos de rede, um com as estações de trabalho e placas internas dos servidores, no outro o roteador e as placas externas dos servidores. Tal layout fragiliza a proteção do *firewall*, uma vez todos os servidores que precisam ser acessados remotamente possuem uma placa externa com endereço IP real, permitindo que um atacante possa explorar uma vulnerabilidade sem ter que passar pela primeira defesa que seria *firewall*.

4.8.4.3 Área física

Apesar de existirem regras para impedir que pessoas não autorizadas tenham acesso a sala dos servidores, não existe um monitoramento do ambiente, criando assim uma falha na segurança, ou seja, pessoas autorizadas podem entrar na sala e atentar contra a segurança da empresa e a equipe de informática não terá como identificar a pessoa que praticou a ação. Outro ponto que foi observado foi à ausência de mecanismos seguros do tipo trancas com leitores de digitais ou qualquer recurso que use biometria.

4.8.5 Proteção dos dados

Proteger os dados no ambiente corporativo não é missão fácil, além de demandar muito tempo é um trabalho bastante tedioso. A equipe de informática usa algumas ferramentas para proteger a empresa contra a perda de dados. Identificamos três grandes volumes de dados que são cuidadosamente protegidos. O primeiro é o material produzido pelos usuários tais como planilha, documentos texto, trabalhos gráficos, pequenas base de dados de softwares de fiscais. O segundo são os e-mails recebidos e enviados, sendo necessário à proteção desse tipo de dado porque quase 100% dos comunicados e das negociações com fornecedores e clientes são feitos via e-mail. A terceira e mais importante massa de dados que é protegida é a base de dados do sistema de gestão corporativo, que possui dados de todas as filiais.

4.8.5.1 Backups

Os backups são feitos diariamente e registrados. As fitas são guardadas no mesmo ambiente onde os backups são realizados. Os backups são controlados através de planilhas que devem ser preenchidas pelo operador do backup e assinado pelo gerente de informática. Os backups da base de dados são testados duas vezes na semana, o que diminui a

possibilidade de falhas no caso de existir a necessidade de realizar uma restauração da base de dados.

4.8.5.2 Energia

A empresa estudada possui um sistema de energia alternativa ou como é conhecido, sistema UPS, altamente eficiente, formado por uma solução de no-breaks com dois nós trabalhando em paralelo, sendo que caso um precise ser desligado por problemas ou para manutenção, o outro assume todo o trabalho. O sistema é todo gerenciado por software e permite que seja feito um monitoramento via Internet. Todo o parque tecnológico é suportado pela solução que segundo levantamos, possui um folga de crescimento de mais de 50%. A autonomia do sistema em carga máxima é de uma hora. A empresa possui um contrato de prestação de serviço para manutenção dos equipamentos, no qual os técnicos estão disponíveis 24 horas por dia e 7 dias por semana.

4.8.6 Telecomunicação

O uso maciço da Internet, a quantidade de aplicações e necessidade de se conectar a filias, clientes e fornecedores, fez com que as empresas passem a trabalhar praticamente 24 horas conectadas a Internet. Do outro lado, a falta ou paralisação dos serviços de telecomunicação podem trazer sérios prejuízos à empresa.

A empresa possui circuitos de telecomunicação que são extremamente vitais ao negócio, uma vez todos os pedidos enviados pelos representantes comerciais são enviados direto para o sistema principal da empresa através desse circuito. Para garantir a continuidade operacional, a empresa possui um outro circuito de dados que em caso de falha do circuito principal, o circuito secundário assumirá. Identificamos também que a empresa possui um mecanismo para acompanhamento das falhas que o sistema de telecomunicação apresenta e qual foi a medida adotada para solucionar. Identificamos como uma falha de segurança a falta de equipamento de telecomunicação sobressalente para que no caso de uma pane em um dos equipamentos o tempo de parada seja mínimo.

4.8.7 Serviços

O principal sistema da empresa é um sistema de gestão integrada, que além da ferramenta de gestão a empresa oferece uma série de recursos que hoje são imprescindíveis em qualquer ambiente como, por exemplo, o correio eletrônico, o acesso à internet via navegador. A empresa possui um sistema próprio de correio eletrônico no qual é usado a tecnologia de correio da Microsoft. A equipe de informática criou um documento com o

objetivo de orientar usuários e ao mesmo tempo informa-los sobre as regras de uso do sistema de correio. Identificamos a utilização de uma serie de restrições que garantem o bom funcionamento do sistema como por exemplo:

- A limitação do tamanho das mensagens;
- A limitação do espaço em caixa postal por usuário;
- O acesso ao sistema de correio, que segundo o procedimento, só é permitido de dentro da organização ou via rede privada.

Identificamos alguns possíveis pontos de vulnerabilidade como, por exemplo:

- O sistema de correio não possuir um filtro ant-spam;
- O sistema se localizar diretamente na rede publica, permitindo que um atacante possa ter acesso direto ao sistema;
- Não existir um sistema alternativo em caso de falha;
- O fato do sistema já esta ultrapassada, uma vez que existem versões mais novas do produto.

O acesso à Internet é provido por um sistema de proxy que além de fazer *caching* para diminuir a tempo de espere, faz controle de acesso baseado em conteúdo, controle de acesso por horário e controle de acesso por usuários e está localizado dentro da rede interna. Por outro lado, não existe um documento formalizado que descreva essas regras, para que os usuários tenham consciência das limitações impostas pelo sistema. Outro ponto que pode ser considerada uma falha é a falta de uma documentação onde sejam descritos quais os parâmetros mínimos de configuração da ferramenta para que no caso de ser preciso reinstalá-lo, não se perca tempo.

4.8.8 Recurso humano

Possuir sistemas altamente sofisticados não é de grande valia se a equipe de informática não estiver apta a explorar o máximo dos sistemas. A capacitação tecnológica é fator fundamental para garantir o sucesso de qualquer projeto, inclusive os relacionados à segurança informação.

Como já dito anteriormente, a empresa não possui um setor ou um profissional exclusivo à segurança da informação, o que acaba dificultando o cumprimento de alguns procedimentos e até mesmo a identificação de novas soluções que possam ajudar a empresa. Porém, é notório o investimento feito pela empresa no que diz respeito à capacitação tecnologia o que acaba deixando a *equipe sempre atualizada. Identificamos treinamentos*

específicos da área de segurança da informação, o que vem a reforçar a idéia de que existe uma preocupação por parte dos altos executivos.

5. CONCLUSÃO

É do nosso conhecimento que a segurança da informação é bastante complexa e que é de muita particularidade, ou seja, varia de empresa para empresa. Sabemos também que a segurança da informação não está baseada em um produto ou em uma solução de mercado, mais em um conjunto de procedimento que são na sua maioria, aplicáveis apenas a uma organização. Este trabalho não teve a pretensão de servir como um guia ou uma referência à projeto de segurança da informação, uma vez que foi direcionado para uma empresa específica, e que acreditamos poder contribuir de alguma forma na melhoria dos processos de segurança por ele utilizada. Assim, gostaríamos de dar algumas sugestões com relação ao que observamos.

A pesar de possuir um sistema de atualização bastante eficiente, seria interessante que as atualizações das estações fossem feitas em horários diferentes, o que não acontece. Essa medida poderá ajudar a empresa evitando que a mesma não tenha sua rede paralisada pela quantidade de *downloads* simultâneos. Outra medida que poderia ajudar bastante era a aquisição se possível de uma estação de teste para que as atualizações fossem baixadas primeiro nessa máquina, diminuindo as chances de acontecer um problemas de atualização mau sucedida em uma máquina de produção.

Os procedimentos de atualizações no hardware garantem que problemas não ocorram, causando a perda de dados, porém, acreditamos ser prudente a criação de mecanismos que sirvam para registrar todo e qualquer trabalho feito nos equipamentos da empresa, principalmente os de missa crítica.

Com relação às contas e senhas, equipe de informática deveria criar uma política onde tivesse escrito todos os cuidados que devem ser tomados na criação de uma conta para um novo funcionário, pois a falta desse tipo de procedimento, pode permitir que no futuro uma pessoa que tem a permissão, porém não recebeu o devido treinamento, crie uma conta que fuja dos padrões.

Como identificado acima, não existe um controle do tráfego que passa por dentro dos túneis VPN, assim, sugerimos que seja liberado apenas o tráfego correspondente ao serviço que estão sendo disponibilizados pela empresa. Tal bloqueio, pode ser feito usando as próprias soluções existentes na empresa que como observado, possui suporte a esse tipo de recurso.

Tanto os problemas do não registro de visitantes à sala de servidores como a não monitoração em tempo real, podem ser facilmente resolvidos, com a utilização de câmeras com tecnologia *wireless* de baixo custo que além de monitorar a sala dos servidores em tempo real, pode substituir o registro de visitantes.

As sugestões com relação à proteção de dados são:

- Comprar uma caixa-cofre para guardar as fitas que ficam no local;
- Manter uma cópia dos backups fora da empresa e se possível, montar uma solução de backup site;
- Manter sempre um disco de reserva para reconstruir o espelhamento.

Sugerimos também a aquisição de um sistema de acesso remoto para prover acesso via VPN discado. Nesse caso, se o link primário ou secundária tiverem problemas, tanto a filial como os representantes poderão acessar a empresa através da VPN discada.

Hoje um dos maiores problemas que as empresas enfrentam são os e-mails indesejados. Como a empresa não possui na solução de correio um mecanismo que possa combater esse tipo de ameaça, sugerimos que seja adotada uma das opções abaixo:

- Substituição da solução atual que já está sendo descontinuada, por uma versão nova do produto que já possui ferramentas para combater o e-mails indesejados;
- Substituir a solução atual por uma de um outro fornecedor que possua as ferramentas necessárias;
- Adquirir um software ou hardware que trabalhe em conjunto da solução atual;
- Comprar um produto que atue no lado cliente, tendo o objetivo de bloquear os e-mails indesejados.

Gostaríamos de sugerir também que todos os servidores (com exceção do servidor de *firewall*) que precisam ser acessados pelo mundo externo ficassem em uma rede intermediária, impedindo que *hackers* tenham acesso a eles sem muita dificuldade.

Identificamos também na organização, traços mostram a preocupação da equipe de informática com a segurança da informação, uma vez que ficou bastante claro a intenção da equipe de continuar a melhorar os processos que dão suporte a segurança da informação.

Acreditamos que mesmo com a identificação de procedimento, ferramentas, recursos tecnológicos e principalmente o comprometimento da equipe de informática, a empresa precisa aprimorar a segurança da informação em seu ambiente, criando para tal, uma política

de segurança da informação coerente com a norma NBR ISO/IEC 17799, criar um plano de contingência que esteja alinhado com o plano de continuidade da empresa e para gerenciar tudo isso, criar um cargo de *security officer*, que como já foi dito acima, tem como seu objetivo principal zelar pela informação da empresa.

Outro ponto importante foi à identificação da preocupação com a segurança da informação em outros setores, o que mostra o trabalho de conscientização que vem sendo feito junto ao usuário final. Por fim, acreditamos que os nossos objetivos foram alcançados, uma vez que conseguimos levantar informações suficientes junto à equipe de informática concluindo que a empresa estudada está de fato no caminho certo quando se fala em segurança da informação, uma vez que faz uso de ferramentas, procedimentos e técnicas que são bastante utilizados por várias empresas que já tratam a segurança da informação há bastante tempo, e o que é mais importante, possui a consciência que a melhoria constante é algo que faz parte de todo e qualquer trabalho de segurança da informação.

6 REFERÊNCIAS BIBLIOGRÁFICA

Assessoria de Informática. Regulamento Geral para uso e Administração de Computadores e Redes da UNESP. Disponível em www.unesp.br/ai. Acesso em 03 de maio de 2004.

CASTRO FILHO, Paulo Farias. A Arte da Sobrevivência na Selva da tecnologia. Rio de Janeiro: Axcel Book, 2003.

CSU, Computer Security Unit. Historia dos Vírus. Disponível em http://www.csu.uem.mz/virus_historia.htm. Acesso em 22 de Junho de 2004.

DIAS, CLAUDIA. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Axcel Book, 2000.

FREIRE, Alexandre. Sistemas de Firewall e Defesa de Perímetros Disponível em www.MÓDULO.com.br. Acesso em 24 de Agosto de 2004.

HAZARI, SUNIL. Firewalls For Beginners. Disponível em <http://www.securityfocus.com/infocus/1182>. Acesso em 29 de Outubro de 2004.

MICROSOFT. Virtual Private Networking in Windows 2000: An Overview. Disponível em: <http://download.microsoft.com/download/9/e/7/9e7f598b-1dfc-4f9f-86f6-3bfe7f2ee884/VPNOverview.doc>. Acesso em 29 de novembro 2004.

NBR ISSO/IEC 17799. Disponível em www.abnt.com.br. Acesso em 21 de Setembro de 2004.

NBSO, NIC BR SECURITY OFFICE. Cartilha de Segurança para Internet. Disponível em: <http://www.nbso.nic.br/docs/cartilha/cartilha-03-privacidade.html#subsec1.1>. Acesso em 20 de Agosto de 2004.

MÓDULO SECURITY. Treinamento em Segurança da Informação. STEP 1. 1 CD-ROM

OLIVEIRA, WILSON JOSE. Segurança da Informação – Técnicas e Soluções. Santa Catarina: Visual Book, 2001.

PELISSARI, F. A. B. Segurança de redes e análise sobre a conscientização das empresas da cidade de Bauru (SP) quanto ao problema. Bauru, 2002. Curso de Especialização em Informática – UNESP, 2002. 112f. Disponível em: <http://www.MÓDULO.com.br/index.jsp>. Acesso em: 27 Julho 2004.

POPPER, Marcos Antonio. Instituto Catarinense de Pós-Graduação – Engenharia Social – Um perigo eminente. Disponível em <http://www.icpg.com.br/artigos/rev03-05.pdf>. Acesso em 03 Setembro 2004.

RAMOS, F. F. Analise de Riscos. Disponível em <http://www.infoguerra.com.br/infonews/talk/1022452321,82492,.shtml>. Acesso em 26 Jun 2004.

RFCs: Disponível em: www.rfc.net. Acesso em: 12 Maio, 2004

SEMOLA, MARCOS. Sua empresa já fez uma análise de riscos de verdade?. Disponível em <http://www.kcl.com.br/newkcl/informativos1.asp?id=159>. Acesso em 26 de Agosto de

2004.

SEMOLA, MARCOS. Você já fez uma análise de riscos de verdade?. Disponível em <http://www.semola.com.br/WebSite99/Frames.htm>. Acesso em 25 de maio de 2004.

SANS, Institute. Intrusion Detection FAQ. Disponível em http://www.sans.org/resources/idfaq/what_is_id.php. Acesso em 08 de maio de 2004.

SYMANTEC SECURITY HANDBOOK. Disponível em <http://enterprisesecurity.symantec.com/SecurityServices/factsheets/esecurityhandbook.pdf>. Acesso em 19 de maio de 2004.