FACULDADE DE MINAS – FAMINAS-BH

CURSO DE SISTEMAS DE INFORMAÇÃO

RUBENS DUTRA GOMES

ANÁLISE E PROPOSTA DE SEGURANÇA DA INFORMAÇÃO EM LABORATÓRIO DE ANATOMIA PATOLÓGICA DE BELO HORIZONTE

BELO HORIZONTE

2008

RUBENS DUTRA GOMES

ANÁLISE E PROPOSTA DE SEGURANÇA DA INFORMAÇÃO EM LABORATÓRIO DE ANATOMIA PATOLÓGICA DE BELO HORIZONTE

Trabalho de Conclusão de Curso apresentado ao Curso de Sistemas de Informação da FAMINAS-BH – Faculdade de Minas, como requisito de avaliação parcial para obtenção do Título de Bacharel em Sistemas de Informação.

Prof. Orientador: Ricardo Terra

BELO HORIZONTE

2008

RUBENS DUTRA GOMES

Título: Análise e proposta de segurança da informação em laboratório de anatomia patológica de Belo Horizonte

Objetivo: Estudar a aplicabilidade de algumas técnicas de segurança da informação em um laboratório de anatomia patológica.

FAMINAS-BH – Faculdade de Minas
Curso de Sistemas de Informação

Área de concentração: Segurança da informação.

Data de aprovação: _____ / _____/ _____

_____

Prof. Ricardo Terra - Orientador

_____

Prof. Paulo Henrique Fernandes de Matos
Coordenador do Curso de Sistemas de Informação
FAMINAS-BH

Dedico este trabalho à minha querida esposa,
pelos momentos em que protelou a realização de seus sonhos
para que visse os meus sonhos realizados.

AGRADECIMENTOS

Meus agradecimentos a Deus que, em sua infinita sabedoria, delineou todo o caminho percorrido, e me fez vislumbrar um horizonte até então desconhecido, sequer imaginado.

À minha querida esposa que, sem medir esforços, contribuiu para que mesmo nos momentos de maior insegurança e, por que não dizer, infortúnio, estava com seu ombro amigo e sua mão estendida, para não me deixar desanimar.

Aos meus pais, que sonharam comigo, planejaram comigo e, hoje, vêem o cumprimento daquilo que eu julgava ser impossível.

Ao professor Ricardo Terra, por seu empenho, dedicação e orientações, sem os quais este trabalho não seria possível.

Aos professores que me levaram ao amadurecimento e me fizeram enxergar um mundo em várias dimensões.

Aos colegas de turma, amigos, pelas diferenças que nos unem e pelos espinhos que fazem com que nos respeitemos e aprendamos a conviver com nossas peculiaridades, sempre juntos, sempre amigos.

Aos amigos da empresa Laboratório Analys Patologia, que motivaram este trabalho, vendo-o como necessário à continuidade do negócio da empresa. Isso demonstra que a empresa empenhará todos os recursos disponíveis para fornecer ao seu cliente um serviço sempre aprimorado, buscando a excelência.

Ao colega Alexandre Delfino Xavier, pela atenção e pela contribuição ao trabalho.

Aos demais amigos, pessoas especiais, que fizeram a diferença nesses anos de lutas, que me suportaram, mesmo quando não podia lhes dedicar toda a minha atenção. Amigos que dividiram o fardo, e que, agora, irão também compartilhar da vitória.

Em especial, ao querido amigo Dr. Nivaldo Hartung Toppa, sempre presente, sempre atencioso, sempre com uma mão estendida para ajudar, mais que amigo, mais que irmão, um pai. À Dra. Lúcia Porto Fonseca de Castro, "*I Love you so, although I don't show*". Ao Dr. Eduardo Paulino Junior, pela atenção e ajuda nos momentos de necessidade.

“Há quem passe pelo bosque e só veja lenha para a fogueira."

Liev Tolstoi

RESUMO

Este trabalho tem por objetivo analisar a situação de segurança atual em um laboratório de anatomia patológica de grande porte da cidade de Belo Horizonte. Nesse ramo, a integridade, a confidencialidade e a disponibilidade da informação são importantes para a manutenção da saúde do cliente e para garantir o sucesso e a continuidade do negócio da empresa. Este estudo apresenta dados sobre segurança de informações e da empresa e as técnicas de segurança aplicadas atualmente à empresa em questão, abrangendo segurança tecnológica, física e humana. Em relação à segurança tecnológica, técnicas computacionais aplicáveis são sugeridas. Em relação à segurança física, são feitas sugestões básicas, porém importantes para conferir um maior nível de segurança às informações, aos servidores de informações e aos funcionários da empresa. Em relação à segurança humana, são feitas sugestões visando proporcionar ao funcionário maior segurança no desempenho de suas funções e prepará-lo para identificar e defender-se de ataques envolvendo a engenharia social. Uma análise posterior foi realizada, baseada na implantação das técnicas sugeridas, com o objetivo de demonstrar a melhoria do nível de segurança das informações.

Palavras-chave: Informação, confidencialidade, integridade, disponibilidade, técnicas de segurança, segurança física, tecnológica e humana.

ABSTRACT

This work has as objective to analyse the situation of real security in a big pathological laboratory in Belo Horizonte. In this area, the information integrity, confidentiality, and availability are important to keep the client health and make sure the success and the continuity of the company in business. This study analyses the information and the company security, and the security techniques applied to the referred company, taking into account the technological, physical and human security. In relation to the technologial security, it is suggested the use of applicable computacional techniques. In relation to the physical security, it is suggested the application of basic procedures, although they are important to give a greater level of security to information, to the information servers and to the company employees. In relation to the human security, suggestions were made in order to provide the employee a greater security during the performance of his work and prepare him to identify and protect himself from attacks involving social engineering. A posterior analysis was made, based on the implementation of the suggested techniques aiming to demonstrate the improvement of the information security level.

Keywords: information, confidentiality, integrity, availability, security techniques, physical, technological, and human security.

LISTA DE ILUSTRAÇÔES

SUMÁRIO

1 INTRODUÇÃO

Constantes avanços de tecnologia têm ocorrido, na tentativa de ajudar a resolver problemas e automatizar processos. A informação tem se tornado fundamental para a vida das pessoas, a cada dia. Conforme Toffler (1990), citado por Cavalcanti (1995, p.1), duas grandes e fundamentais mudanças aconteceram, na história da humanidade. A primeira, cerca de 10.000 anos atrás, foi a Revolução Agrícola. A segunda, a Revolução Industrial, ocorreu após 1776, com a invenção da máquina a vapor. Outra grande mudança, ainda em curso, a Revolução da Informação, é configurada pelos avanços da tecnologia e das telecomunicações.

Assim como, na era industrial, a associação de terra, trabalho e capital eram as formas de criar riqueza, na era atual, o mais importante recurso de se agregar valor é a informação. Segundo Dias (2000), citada por Laureano (2005), a informação é o patrimônio mais importante das empresas. Sêmola (2003), citado por Peixoto (2005), afirmou que a informação é um ativo crítico para a continuidade dos negócios de uma empresa e representa a inteligência competitiva dos negócios. Além disso, conforme Laureano (2005), a sociedade atual se baseia em informações, de forma que, cada vez mais, elas são coletadas, armazenadas e utilizadas para que as organizações tenham maior êxito em suas operações.

Se, no mundo físico, existem pessoas tentando obter alguma vantagem sobre outras de formas ilícitas, no mundo virtual, também existem, com a possibilidade de utilizar processos automatizados e, assim, tornar o problema maior ainda, conforme Schneier (2001). Segundo Scheinkman (2006, p.1), Willie Sutton, famoso assaltante de bancos norte-americano da primeira metade do século XX, assaltava bancos porque era lá onde o dinheiro estava. Hoje em dia, é a informação que é muito cobiçada, tornando-se tão ou mais desejada que o próprio dinheiro. Então, sempre há pessoas interessadas em tirar vantagem sobre outras, utilizando-se dessas informações. Assim como Willie Sutton roubava bancos, há pessoas que, a todo tempo, trabalham no intuito de roubar informações, porém com o agravante de poder automatizar essas tentativas através de técnicas computacionais. Um fator agravante para a situação é que, na maioria das vezes, nossas informações estão desprotegidas ou expostas a ataques ou perdas não intencionais.

Não se devem confundir os conceitos de “dados” e “informações”. Segundo Ferreira (2004), “dado” pode ser entendido como a base para a formação de um juízo, um elemento da informação, ou representação de fatos ou instruções. Por outro lado, “informação” é a “coleção de fatos ou de outros dados fornecidos à máquina, a fim de se objetivar um processamento” (FERREIRA, 2004). Então, entende-se que as informações são resultado do processamento dos dados coletados, e a interpretação dessas informações irá gerar o conhecimento.

Um laboratório de anatomia patológica é uma empresa dedicada à realização de exames médicos de citopatologia (preventivo do câncer do colo uterino, também chamado de Papanicolaou), anatomia patológica (biópsias, revisões de casos, exames de líquidos corporais) e imunoistoquímica. Nesses exames, são trabalhadas informações muito importantes, que dizem respeito somente ao paciente, de acordo com definição de Andrade e Silva (2002). Então, essas informações devem ser mantidas em segurança, íntegras e somente disponíveis para pessoal autorizado. No caso da empresa analisada, qualquer perda de integridade da informação poderia acarretar à empresa o encerramento de suas atividades, bem como a suspensão do registro do responsável técnico no conselho de classe correspondente. Além disso, poderia provocar ao cliente danos graves, que poderiam ser fatais. Um paciente necessita de suas informações disponíveis no momento da solicitação. Ao trabalhar com informações importantes, devem-se ter alguns cuidados, pois as informações são confidenciais e dizem respeito somente ao cliente. Na tentativa de conferir um nível adequado de segurança às informações, três objetivos são fundamentais: confidencialidade, integridade e disponibilidade.

De acordo com Araújo (2007), confidencialidade é a garantia de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização. A confidencialidade garante que somente pessoas autorizadas poderão ter acesso à informação. Além disso, determina os níveis de acesso a diferentes tipos de informação. Essa característica é muito importante na empresa analisada, pois a saúde do paciente é algo que diz respeito somente a ele.

A integridade é definida pelo mesmo autor como a propriedade de proteção à precisão e perfeição de recursos. A informação, além de ter o acesso controlado, necessita estar íntegra, para que o usuário autorizado tenha informações confiáveis com que possa trabalhar. Para tanto, deve-se prover meios de se evitar que a informação seja indevidamente alterada ou excluída, seja nos sistemas de arquivo,

seja no caminho percorrido entre o remetente e o destinatário da informação. Como a informação do paciente é muito importante para a manutenção de sua saúde, é necessário que essa informação esteja íntegra, para garantir que o profissional assistente terá informações corretas que irão possibilitar a escolha do tratamento adequado a cada caso.

Além de confidencial e íntegra, a informação necessita estar disponível. A disponibilidade é definida como a característica de ser acessível e poder ser utilizada sob demanda por entidade autorizada. Afinal, “de nada adiantaria termos a confidencialidade e a integridade se tais informações não estiverem disponíveis para serem acessadas.” (PEIXOTO, 2006, p.39). Um paciente necessita de suas informações disponíveis, para que a conduta terapêutica adequada seja adotada.

Porém, aplicar à informação somente os três princípios citados não garante que a informação esteja segura. Segundo Peixoto (2006), ainda devem ser feitos questionamentos quanto à segurança física, segurança tecnológica e segurança humana, sendo que essa última merece destaque especial.

A área onde geralmente mais se investe, quando se trata de segurança da informação, é a tecnológica. Trata-se da aplicação de técnicas de segurança, tais como as citadas abaixo:

- *Firewall*: “sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes” (ABNT NBR ISO/IEC 17799:2005, p.7).
- *Proxy*: conforme Laureano (2005), um tipo de *firewall*, porém controla a conexão a serviços em rede.
- *IDS (Intrusion Detection System,* ou Sistema de detecção de intrusos em português): técnica que objetiva identificar tentativas de invasão a algum computador ou à rede de computadores, conforme traduzido por Laureano (2005).
- Antivírus: de acordo com Silva, Carvalho e Torres (2003), aplicação para detecção de vírus, que pode ser baseada em assinaturas ou em comportamento. Antivírus baseados em assinaturas fazem uso de trechos de código comum a diversos programas maliciosos para identificar possíveis problemas. Antivírus baseados em comportamento analisam programas e a interação deles com o sistema, a fim de identificar possíveis infecções virais.

No capítulo 2, item 2.1, além dessas técnicas de segurança, muitas outras serão analisadas, para maior compreensão das várias possibilidades de proteção à informação.

A norma ABNT NBR ISO/IEC 17799:2000 diz que convém proteger as instalações e informações da organização contra o acesso não autorizado, danos e interferência, de acordo com os riscos identificados. Além de tecnologia em nível de software, é necessário garantir o meio onde os sistemas de software estarão sendo executados e, assim, construir um ambiente mais seguro. E isso não se refere apenas à informática. Em qualquer situação, são necessários investimentos em segurança física para proteger contra os riscos já citados. A segurança física será abordada em detalhes na seção 2.2 do capítulo 2.

Porém, Silva, Carvalho e Torres (2003) afirmaram que, em alguns casos, a maior ameaça aos sistemas são as pessoas que têm acesso às informações, algumas vezes por atitudes criminosas, outras por descuidos ou falta de preparação para tratar a informação de maneira segura. Daí, a necessidade de investimentos em segurança humana. A segurança humana e a engenharia social serão abordadas em detalhes na seção 2.3 do capítulo 2.

Este trabalho estuda a aplicabilidade de algumas dessas técnicas de segurança da informação em um laboratório de anatomia patológica. Com início em Agosto de 2008, essa análise ajudará a empresa a nortear seus investimentos em segurança da informação, para que as informações trabalhadas na empresa, que são vitais para o negócio, não estejam muito expostas a ataques e invasões.

Percebeu-se a necessidade da empresa em conferir um nível adequado de segurança às suas informações. A empresa já foi vítima de engenharia social, indisponibilidade e dados não confiáveis. Optou-se por fazer pesquisa de campo, analisando a empresa e o contexto no qual ela se encontra na sociedade e no segmento do qual faz parte: a saúde.

A partir disso, um acompanhamento dos mecanismos utilizados na transmissão das informações em toda a empresa se iniciará, para verificar sua adequabilidade. Com base nas observações feitas durante esse acompanhamento, serão indicados os pontos frágeis no processo produtivo.

As observações serão analisadas e, então, serão estudadas técnicas aplicáveis aos processos da empresa, de maneira que as informações sejam trabalhadas com um nível adequado de segurança. As técnicas que melhor se

adequarem às necessidades da empresa serão sugeridas e, a critério da diretoria, serão implementadas nos processos em que se fizerem necessárias.

Ao final, serão feitas novas observações sobre os processos, verificando se as informações e o processo produtivo da empresa podem ser considerados seguros.

2 SEGURANÇA DA INFORMAÇÃO

Conforme Laureano (2005), desde o início da humanidade, há a preocupação com as informações e com o conhecimento atrelado a elas. No Egito antigo, conforme Schneier (2001), para que as informações fossem protegidas e o conhecimento secreto fosse perpetuado, eram escritos hieróglifos[1] fora do padrão.

Com o advento dos computadores, mais de uma pessoa poderia acessar as informações ao mesmo tempo, gerando uma maior preocupação com a questão da segurança da informação. O não gerenciamento do acesso às informações poderia acarretar em acesso não autorizado às informações, caracterizando o chamado "Problema clássico de computadores". A primeira sugestão da época era a construção de um sistema operacional mais aprimorado, mas ainda não havia conhecimento disponível para isso.

Então, nos Estados Unidos, em 1967, iniciou-se o processo oficial de elaboração de um conjunto de regras para a segurança de computadores, por parte do Departamento de Defesa dos Estados Unidos. Além disso, a Agência Central de Inteligência norte-americana iniciou o desenvolvimento do primeiro Sistema Operacional em que se implementavam essas políticas de segurança, nomeado ADEPT-50.

Entre 1970 e 1980, de acordo com Schneier (2001), o Departamento de Defesa dos Estados Unidos custeou inúmeros modelos teóricos para tratarem da segurança da informação, chamados de sistemas de segurança multinível. O mais famoso deles é o modelo Bell-LaPadula, criado em 1975, que definiu a maioria dos conceitos de controle de acesso. Paralelamente, conforme citado por Gonçalves (2003), era desenvolvido pelo coronel Roger R. Shell, o conceito de "kernel seguro", com objetivo de conferir segurança à camada mais interna do sistema operacional.

Em 1977, o Departamento de Defesa norte-americano iniciou trabalhos que culminaram na criação de um conjunto de regras conhecido como "*The Orange Book*", ou, "O Livro Laranja", apelido justificado pela cor da capa do manual. Na realidade, o documento chamava-se "Critérios de Avaliação de Sistema de Computador Confiável do Departamento de Defesa dos Estados Unidos", porém o

[1] Hieróglifo, ou hieroglifo, é a notação utilizada no processo de escrita do Egito antigo, conforme Ferreira (2004).

título era muito longo e logo caiu em desuso. O trabalho de escrita foi terminado e, em 1985, o documento foi publicado pela *National Computer Security Center* (Centro Nacional de Segurança de Computadores), ramificação da *NSA* (agência nacional de segurança norte-americana). De acordo com Gonçalves (2003), esse manual é considerado o precursor dos padrões de segurança.

Em 1987, no Reino Unido, o DTI (*Department of Trade Center,* traduzido por Departamento Central de Comércio) criou o CCSC (*Commercial Computer Security Centre*, traduzido por Centro Comercial de Segurança de Computadores), para auxiliar empresas britânicas que concebiam critérios para avaliação de segurança tecnológica. Em 1989, foi publicada a primeira versão do código de segurança denominado "PD0003 – Código para Gerenciamento de Segurança da Informação".

Segundo Silva, Westphall e Westphall (2003), em 1987, foi criado o modelo de Clark-Wilson e, em 1989, o modelo da Muralha da China. Posteriormente, os canadenses criaram um documento denominado "Critérios Canadenses de Avaliação de Produtos de Computador Confiáveis". Em 1995, surgiu na Europa o documento "Critérios de Avaliação de Segurança da tecnologia da Informação". Então, os norte-americanos criaram os "Critérios Federais", outro documento com normas de segurança da informação.

Na década de 90, houve um esforço em produzir uma padronização mundial. Esse esforço é citado por Schneier (2001) como "Critérios Comuns", gerando a norma ISO 15408, versão 2.1. No empenho da obtenção de um padrão mundial mais atual, que não se detivesse somente na proteção dos computadores, mas em toda forma de informação, foi construída a norma "*BS7799 – Code of Practice for Information Security Management*" (Códigos e Práticas para Configurações de Segurança de Informações). Em 1996, a norma foi proposta ao ISO para homologação, sendo rejeitada. Em 1997, o documento foi novamente revisado, sendo ampliado e publicado em 1998 como BS7799-2:1998.

Em outubro de 2000 é aceita a norma ISO/IEC 17799:2000 na reunião do comitê ISO em Tóquio, capital japonesa. Em setembro de 2001, é homologada a versão brasileira da norma. Desde então, ela tem sido o padrão utilizado por aqueles que desejam elevar o nível de segurança de suas informações.

2.1 Segurança Tecnológica

Nesta seção, segurança tecnológica é descrita como sendo a segurança de hardware e software. É a parte da segurança da informação que geralmente recebe mais investimentos. Diversas técnicas podem ser combinadas, de acordo com a necessidade de proteção da informação, para formar uma solução adequada a cada caso. Eis a descrição de algumas técnicas de segurança tecnológica.

2.1.1 Firewall

Literalmente, “parede de fogo”, porém compreendido como “parede corta-fogo”. Os primeiros *firewalls* estavam nos trens que, na época eram movidos a carvão e, portanto, necessitavam de um enorme forno e grandes quantidades de carvão. Quando o maquinista abastecia de carvão a fornalha, era criada uma nuvem de pó de carvão altamente inflamável. Depois da morte de muitos passageiros nos trens, esses passaram a ser fabricados com paredes de ferro fazendo separação entre o vagão onde se encontrava a fornalha e os vagões de passageiros.

Conforme Laureano (2005), como técnica computacional, um *firewall* funciona como barreira que separa a rede interna, tida como segura, e uma rede externa não confiável. As primeiras técnicas de *firewall* para computadores e redes de computadores, conforme citado por Schneier (2001), eram utilizadas com o objetivo de se isolar problemas dentro de segmentos da rede, evitando que esses problemas se espalhassem por toda a rede. Isso ocorria porque as redes eram problemáticas e paralisavam muitas vezes, causando prejuízos.

Atualmente, o *firewall* atua bloqueando acessos externos indevidos e gerenciando conexões. Segundo Peterson (2004), existem duas categorias de *firewall*: baseado em filtro de pacotes e baseado em *proxy*. O primeiro é o mais utilizado e utiliza regras pré-estabelecidas e gerencia cada pacote de dados que trafega pela rede, permitindo ou não sua passagem. O segundo gerencia a comunicação entre redes de computadores. As aplicações de *proxies* variam desde

a filtragem de pacotes que trafegam entre as redes até o armazenamento temporário de páginas da Internet, tornando mais rápida a navegação.

2.1.2 Antivírus

De acordo com Silva, Carvalho e Torres (2003), são sistemas que vasculham arquivos periodicamente em busca de mudanças não esperadas, em qualquer programa ou arquivo, ou de assinaturas de vírus, que são padrões de códigos utilizados pelos vírus na sua propagação.

As aplicações antivírus mais utilizadas na detecção de vírus baseiam-se em assinaturas para cumprir a sua função. Uma assinatura é um trecho de código binário que permite a identificação do vírus em questão por um simples processo de comparação. Essas soluções obrigam a permanente atualização das bases de dados de assinaturas.

Existem antivírus que, conforme Beal (2005), além das funcionalidades citadas, ainda monitoram o funcionamento dos programas executados no computador, emitindo alertas caso algum programa apresente comportamento suspeito.

2.1.3 Zona desmilitarizada

De acordo com Schneier (2001), é uma zona onde são colocados os arquivos públicos, que não são colocados no *firewall* devido ao risco de ataques ou fora dele porque o risco pode ser maior ainda. Então, coloca-se entre dois *firewalls*, um protegendo a zona desmilitarizada da rede externa e outro protegendo a rede interna da zona desmilitarizada. Como resultado, têm-se uma parte semi-pública e outra mais privada da rede.

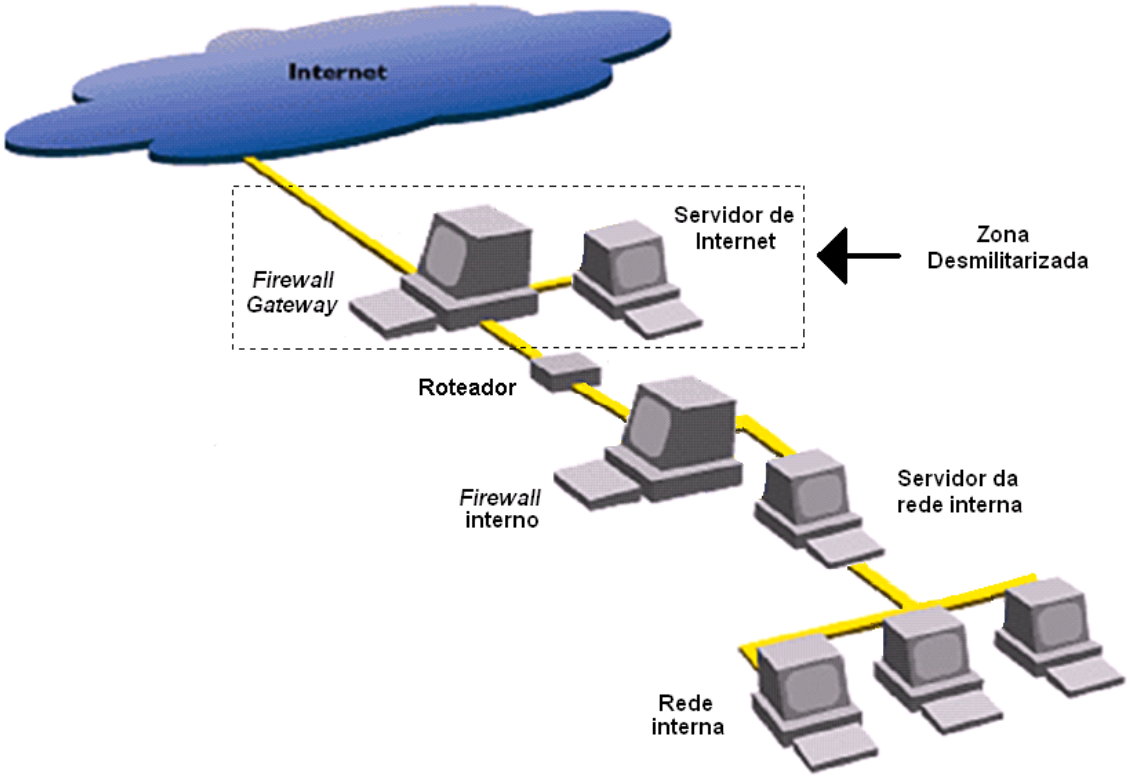

FIGURA 1: Zona Desmilitarizada.
Fonte: Adaptado de PINHEIRO, 2004.

Conforme ilustrado na Figura 1, o servidor de Internet está ligado a um *firewall gateway*, por onde entrarão e sairão todas as conexões. Porém, o servidor da rede interna está atrás de outro firewall, protegido de possíveis ataques.

2.1.4 Sistemas de detecção de intrusos

Conforme Schneier (2001), são sistemas que monitoram a rede, procurando comportamento suspeito de arquivos ou programas. Para isso, eles devem conhecer formas de ataque e comportamentos esperados na rede de computadores. Esse comportamento suspeito detectado pode ser a ação de um atacante, tentando ter acesso não autorizado à rede. Então, diante de algum problema identificado, é gerado um alerta, sugerindo uma ação defensiva. Algumas vezes, os sistemas detectam ataques em curso e, em outras, ataques bem-sucedidos. O maior problema com esse tipo de sistema são os alarmes falsos, porém os sistemas de

detecção de intrusão estão passando por constantes aperfeiçoamentos, na tentativa de se obter produtos com mais qualidade e melhor desempenho.

2.1.5 Criptografia

De acordo com Schneier (2001), é um conjunto de conceitos e técnicas utilizado para transformar uma informação legível em outra ilegível, a menos que seja conhecida uma chave secreta utilizada na cifragem. Dessa forma, ao menos teoricamente, somente o emissor e o receptor da mensagem terão livre acesso a ela. Existem dois tipos de criptografia: simétrica e assimétrica.

Na criptografia simétrica, são utilizados algoritmos de cifragem e decifragem com uma só chave (a mesma que cifra, também decifra a mensagem) como uma senha, ou duas chaves relacionadas, podendo até mesmo ser, uma delas, a transformação da outra. Caso seja usado apenas uma chave, remetente e destinatário devem ser conhecedores da chave. Caso duas, deve ser estudada uma maneira segura de fazer conhecer ao destinatário a chave a ser usada. É um método bem simples, porém menos seguro, pois, caso haja grande quantidade de pessoas envolvidas nas transmissões, poderá haver necessidade de criação de uma grande quantidade de chaves diferentes. Além disso, deve ser providenciado um método seguro de armazenamento e transporte dessas chaves, para não permitir que pessoas não autorizadas as utilizem. Caso isso ocorra, pode ser necessária a troca de todas as chaves. Porém, como são mais simples, os algoritmos de chave simétrica possuem melhor desempenho que os algoritmos de chave assimétrica.

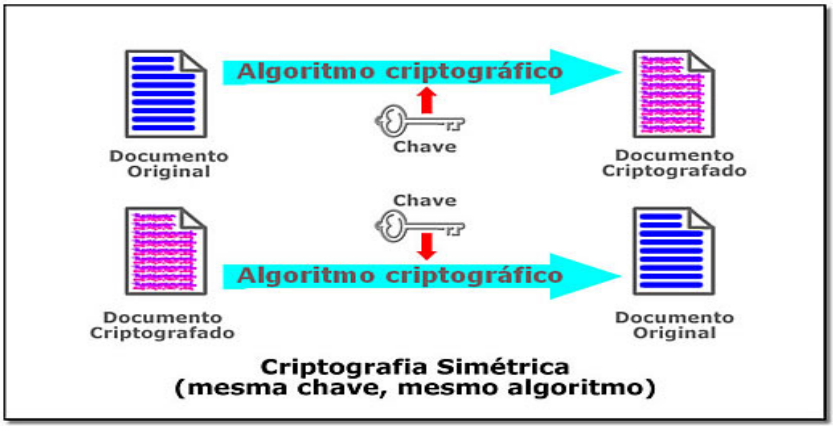

FIGURA 2: Representação de criptografia simétrica.

Fonte: PIROPO, 2007.

Conforme ilustrado na Figura 2, uma chave é utilizada em um algoritmo criptográfico para cifrar um documento original, transformando-o em um documento criptografado, ou documento cifrado. Então, a mesma chave é utilizada pelo algoritmo criptográfico para decifrar o documento, permitindo o acesso ao documento original.

Criptografia assimétrica é o processo em que são utilizadas duas chaves distintas: uma pública e uma privada. As duas chaves são diferentes entre si e, conforme Schneier (2001), não é possível calcular uma chave a partir da outra. Dessa forma, quando um emissor “A” quiser enviar uma mensagem, deverá cifrá-la com sua chave privada. Um receptor “B” deverá ter uma cópia da chave pública do emissor, para possibilitar a leitura da mensagem. Somente quem tiver uma cópia da chave pública do emissor poderá ler a mensagem. E, caso a operação seja inversa, e “B” quiser enviar uma mensagem para “A”, poderá cifrá-la com a chave pública de “A” e, quando “A” receber a mensagem, a abrirá com sua chave privada.

Ainda conforme Schneier (2001), a criptografia assimétrica não é utilizada para codificar mensagens, devido ao baixo desempenho quando comparada à criptografia simétrica. No entanto, é utilizada uma técnica híbrida, utilizando-se uma chave aleatória criada no momento da cifragem da mensagem (chamada “chave de sessão”). Assim, a mensagem é cifrada por criptografia simétrica utilizando-se a chave de sessão e esta é codificada utilizando-se criptografia assimétrica, através da chave do emissor. O receptor da mensagem deverá utilizar sua chave para decifrar a chave de sessão e, então, esta será utilizada para decifrar a mensagem. Essa é uma técnica utilizada por grande parte dos sistemas operacionais.

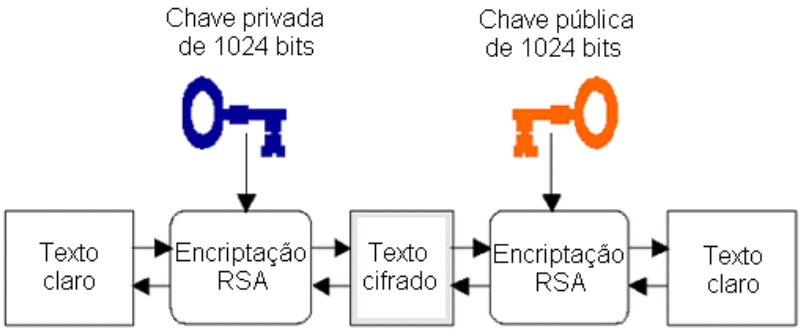

FIGURA 3: Representação de criptografia assimétrica.

Fonte: Adaptado de RAPOPORT, 2003.

Conforme ilustrado na Figura 3, um texto qualquer, chamado de “texto claro”, é encriptado ou cifrado utilizando-se o algoritmo RSA e a chave pública do destinatário, com tamanho de 1.024 bits. Então o destinatário, utilizando o algoritmo RSA e a sua chave privada, decifra o texto obtendo novamente o texto original.

Diversos tipos de algoritmos de criptografia são utilizados, entre eles o RSA, El-Gamal, DSA, DES, DES triplo, IDEA, RC, AES e o Blowfish. Algumas empresas criam seus próprios algoritmos de criptografia, porém, segundo Schneier (2001), os algoritmos criptográficos mais interessantes são os algoritmos de domínio público.

Conforme Laureano (2005), o RSA é um sistema criptográfico de chave pública que utiliza criptografia em blocos e possui uma segurança considerável, devido à alta complexidade de uma chave RSA. A chave pode ser de qualquer tamanho. Embora alguns acreditem que quanto maior a chave, maior a segurança, segundo Schneier (2001) também devem ser observados a entropia e a qualidade do algoritmo criptográfico. A entropia, medida de incerteza, refere-se às senhas mais prováveis. O algoritmo criptográfico deve escolhido de forma que atenda às necessidades de cada caso, porém deve-se certificar que ele utiliza corretamente a entropia prometida na chave criptográfica, garantindo a qualidade do algoritmo.

2.1.6 Certificado

De acordo com Peixoto (2005), é um arquivo que contém um conjunto de informações a serem enviadas juntamente com a mensagem cifrada. As

informações mais comuns em um certificado são:

- Informações referentes à entidade para a qual o certificado foi emitido (nome, e-mail, CPF/CNPJ, PIS, etc);
- Chave pública referente à chave privada de posse da entidade especificada no certificado;
- Período de validade do certificado;
- Localização do "centro de revogação";
- Assinatura da Autoridade Certificadora que afirma que a chave pública contida naquele certificado confere com as informações contidas no mesmo.

A utilização de certificados garante a origem dos dados, não permitindo que dados de origem duvidosa circulem pela rede de computadores. Além disso, permite a verificação da integridade dos dados, garantindo um maior nível de confiabilidade aos dados, protegendo contra alterações não autorizadas.

O certificado X.509 é um dos padrões de certificado, reconhecido internacionalmente. Ele contém as seguintes informações:

- Versão do certificado;
- Número serial - todo certificado possui um. Este número não é globalmente único, mas único no âmbito de uma Autoridade Certificadora. As listas de certificados revogados utilizam esse número serial para apontar quais certificados se encontram revogados;
- Tipo de algoritmo criptográfico utilizado pela Autoridade Certificadora para assinar o certificado, juntamente com o tipo de função criptográfica usada no certificado;
- Nome do titular para o qual o certificado foi emitido;
- Nome do emitente - Autoridade Certificadora que emitiu/assinou o certificado;
- período de validade do certificado, no formato "Não antes de" e "Não depois de";
- Informações de chave pública da entidade, a saber:
    - Algoritmo de chave pública;
    - A própria chave pública.
- Assinatura da Autoridade Certificadora - a garantia sobre a veracidade das informações contidas no certificado, de acordo com as políticas da própria

Autoridade Certificadora;

- Identificador da chave do titular - é uma extensão do X.509 que possui um identificador numérico para a chave pública contida no certificado, especialmente útil para que programas de computador possam se referir a ela;
- Identificador da chave do emitente - a mesma idéia mencionada anteriormente, só que se referindo a chave pública da Autoridade Certificadora que emitiu o certificado.

2.1.7 Esteganografia

Segundo Schneier (2001), é a técnica de se esconder uma mensagem dentro de outra mensagem. Por exemplo, pode-se colocar um texto criptografado dentro de um arquivo de imagem. A esteganografia não pode ser confundida com a criptografia, pois, enquanto a esteganografia esconde a mensagem em si, a criptografia esconde o significado da mensagem. Dessa forma, o receptor deverá conhecer essa técnica e utilizar programas que consigam ler a mensagem oculta, fornecendo uma chave secreta para isso.

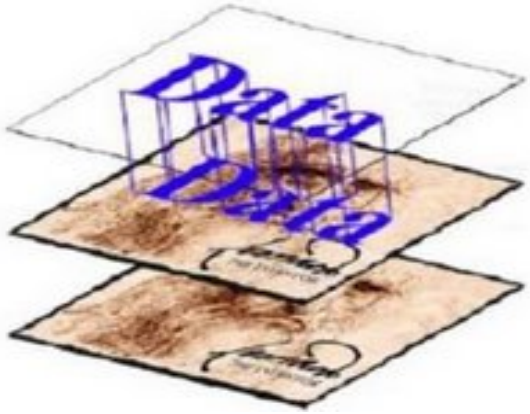

FIGURA 4: Representação de esteganografia.
Fonte: AGREDA, 2008.

Na Figura 4, é demonstrado que um dado qualquer, no caso um texto, pode ser ocultado em uma figura qualquer e não ser visto, a não ser utilizando-se

programas específicos.

Segundo Bustamante (2006), a esteganografia é utilizada desde o século V a.C. Histio necessitava contactar secretamente seu superior, Aristágoras de Mileto. Então, convocou um servo em quem confiava, raspou-lhe cabeça, desenhou uma mensagem e o mandou ao encontro de Aristágoras. Durante a longa viagem os cabelos do escravo cresciam permitindo que a mensagem estivesse devidamente escondida. Ao chegar à presença de Aristágoras de Mileto, o escravo deveria raspar novamente a cabeça perante Aristágoras, para que ele pudesse ler a mensagem secreta.

Atualmente, a esteganografia é amplamente utilizada na confecção de cédulas monetárias. Alguns detalhes ocultos são visíveis somente através de equipamentos apropriados, lentes ou reagentes.

Figura 5: Exemplo de esteganografia.
Fonte: BUSTAMANTE, 2006.

Na Figura 5, é ilustrada uma cédula financeira, em que existe intensa aplicação de técnicas esteganográficas para garantir a sua autenticidade.

A esteganografia pode ser utilizada em textos, áudio, vídeo, imagens e até mesmo em pacotes TCP/IP, exigindo que o responsável pela segurança da rede de computadores aplique rotinas de verificação minuciosa de dados em arquivos ou na memória, apagados ou não, cifrados ou até mesmo danificados, sem descartar nenhuma possibilidade.

2.2 Segurança Física

Conforme Laureano (2005), o principal objetivo da implantação de controles de segurança física é restringir o acesso às áreas críticas da organização, prevenindo contra acessos não autorizados, que podem acarretar danos a equipamentos, acesso indevido à informação, roubos de equipamentos, entre outros. Restringir o acesso aos equipamentos da empresa utilizando apenas senhas nos computadores pode não ser suficiente, uma vez que um atacante poderia levar o equipamento consigo.

Os controles de acesso físico devem ser implementados em conjunto com os controles de acesso lógico. Além de portas e fechaduras, podem ser utilizados leitores biométricos ou dispositivos que solicitem senhas de acesso, além de liberação de acesso pelo perfil do colaborador. Algumas soluções de controle de acesso combinam autenticação biométrica e chaves especiais, outras combinam a utilização simultânea de duas chaves diferentes.

Existem diversas ameaças com as quais uma empresa deve se preocupar. Contudo, merecem destaque as seguintes ameaças:

- Incêndio: a empresa deverá dispor de várias classes diferentes de extintores de incêndio, possibilitando debelar pequenas chamas, caso existam;
- Água: deverá existir proteção contra vazamentos ou enchentes, elevando os equipamentos em um nível acima da água;
- Sabotagem e vandalismo: deve ser providenciada solução para proteger a empresa de sabotagens, com planos auxiliares de trabalho, além de canais de contato com autoridades policiais locais;
- Roubos e furtos: devem ser implementadas técnicas que garantam que, mesmo que a empresa sofra ação de malfeitores, o negócio seja retomado e a produção sofra o menor impacto possível;
- Interrupção de energia ou de comunicações: devem-se prover meios que garantam a operacionabilidade da empresa, mesmo em situações de adversidade, como falta de energia e interrupção de canais de comunicação de dados e voz. Para tanto, podem ser utilizados geradores de energia e canais alternativos de comunicação.

- Falhas em equipamentos: deve-se possuir um planejamento de manutenções preventivas nos equipamentos para evitar paradas inesperadas de produção devidas a falhas em equipamentos. Caso não seja possível, a empresa deve contar com mecanismos de substituição de equipamentos, acarretando ao processo produtivo o menor impacto possível.

2.3 Segurança Humana

Conforme Peixoto (2005), o fator humano está associado à maioria dos sucessos ou dos fracassos, no que se refere à segurança da informação. Kevin Mitnick, um dos mais famosos praticantes de engenharia social do mundo, afirma que aproximadamente 50% das invasões ocorrem principalmente por falha humana. Em muitos casos, problemas não ocorrem por descuido ou premeditação do usuário, mas por falta de informação. Então, justifica-se a capacitação do colaborador, a fim de se ter nele um aliado nos processos que envolvem informações. Entre as opções de capacitação estão palestras de motivação, cursos de atualização profissional, palestras ou mini-cursos de conscientização sobre a importância da informação para o negócio da empresa e palestras sobre engenharia social.

A engenharia social é definida por Peixoto (2003) como a arte de enganar pessoas. O praticante da engenharia social faz uso de diversas ferramentas para conseguir seus objetivos, sejam bons ou ruins. Entre elas, podem ser citados a Internet[2] (através de coleta de dados), acesso remoto indevido via intranet, correspondência eletrônica falsa, e pessoalmente, utilizando técnicas de persuasão e habilidade em saber conversar. O engenheiro social persegue informações que julga serem valiosas. O engenheiro social utilizará todos os métodos de que ele dispuser para obter as informações desejadas. Para tanto, o profissional deve estar preparado para saber identificar possíveis ataques de engenharia social e como agir nessas situações, sem informar o desejado pelo atacante.

[2] Conforme Ferreira (2004), Internet é qualquer conjunto de redes de computadores conectadas entre si por roteadores e *gateways*.

3 ESTUDO DE CASO

3.1 Empresa

Em 1983, o Laboratório Padre Eustáquio foi adquirido pelos Drs. Hélio Gomes Guimarães e Nivaldo Hartung Toppa. Esse nome ficou mantido apenas como razão social, sendo o nome Analys e sua logomarca criados no ano de 1989. Após assumir a direção do Laboratório, houve um incremento significativo do número de exames e o espaço da empresa começou a se demonstrar insuficiente, face à nova demanda.

Em 1985, o laboratório mudou-se para outro imóvel mais amplo. Entre as décadas de 80 e 90, foram abertos postos de coletas em pontos estratégicos na região metropolitana de Belo Horizonte. Em 1995, os setores de Anatomia Patológica e Citopatologia e de Bacteriologia foram transferidos para outro imóvel, ainda maior, para o atendimento da crescente demanda de serviços.

O grande avanço tecnológico e a criação de novos exames fizeram com que o Analys adquirisse aparelhos modernos para realização de exames em medicina ocupacional, endocrinologia, imunologia, hematologia, entre outros.

Em meados de 2005, houve uma separação entre as áreas de anatomia patológica e citopatologia e de patologia clínica. O Dr. Hélio Gomes Guimarães assumiu inteiramente a área de patologia clínica, mantendo o nome “Laboratório Analys Ltda”, enquanto o Dr. Nivaldo Hartung Toppa, diretor das áreas de anatomia patológica e citopatologia, fundou a empresa “Laboratório Analys Patologia Ltda”, objeto de nosso estudo.

Exames referentes à anatomia patológica são realizados exclusivamente por médicos patologistas, enquanto exames referentes à citopatologia podem ser realizados por médicos patologistas, bioquímicos ou citotécnicos, que são profissionais especializados, porém de nível técnico.

Esses exames são interpretativos. Então, para que seja realizada uma análise correta do exame do paciente, é necessário disponibilizar o máximo de informação possível. Através das informações fornecidas e de posse do exame que o profissional está analisando é que se poderá contribuir para o diagnóstico do paciente e, então, fornecer tratamento adequado a cada caso.

Como o trabalho é baseado em informações fornecidas pelo paciente e por seu médico assistente, é fundamental que essas informações estejam disponíveis, e que sejam confiáveis e íntegras. Assim, é muito importante que sejam asseguradas condições de segurança a essa informação. A seguir, será abordada a aplicabilidade de cada uma das técnicas de segurança na empresa, abordando sua viabilidade de implantação.

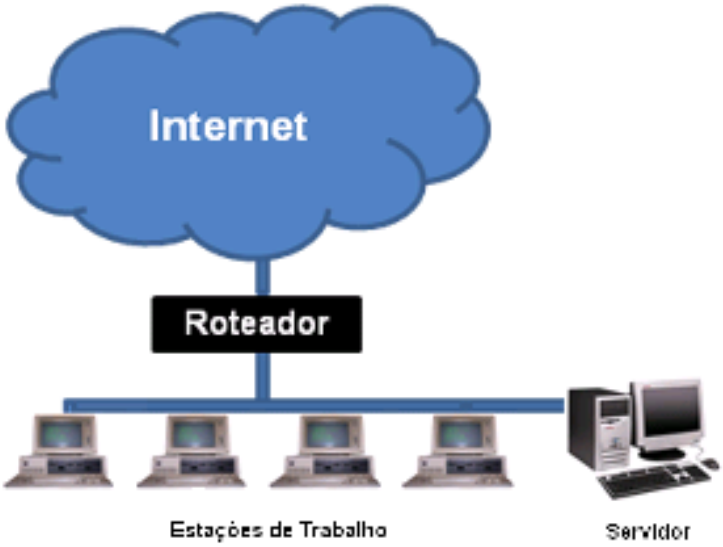

FIGURA 6: Situação da segurança tecnológica na empresa antes das sugestões deste trabalho.
Fonte: Arquivo pessoal.

Conforme ilustrado na Figura 6, a empresa atualmente conta com um roteador, conectando a rede pública com a rede interna de computadores e diversas estações de trabalho conectadas a um servidor geral. O servidor é conectado à rede como um computador comum, sem qualquer cuidado especial.

3.2 Segurança Tecnológica

A empresa não efetua grandes investimentos em tecnologia. Alguns computadores obsoletos, outros com defeitos, impressoras não apropriadas às demandas e sistemas desatualizados fazem com que ocorram paradas inesperadas por mau funcionamento, prejudicando os processos produtivos da empresa.

Portanto, para possibilitar maior disponibilidade das estações de trabalho, fazendo com que as tarefas não sofram interrupções não programadas, é necessário que a empresa faça constantes investimentos em segurança tecnológica, tais como aquisição de computadores de última geração, sistemas operacionais atualizados e manutenções periódicas.

3.2.1 Firewall

A empresa não possui *firewall*. Os funcionários utilizam livremente a Internet para acessar correspondências eletrônicas, *sites* de bate-papo, *sites* de relacionamento ou qualquer outro tipo de conteúdo. O servidor da empresa está obsoleto, contudo operando com sistema operacional de grande porte voltado a grandes servidores. Isso não garante a disponibilidade necessária dos dados, além de provocar lentidão na resposta das solicitações dos computadores da rede.

Nas estações de trabalho situadas fora da matriz da empresa, a comunicação ocorre através de remessas de dados transportadas em discos de dados.

Sugere-se a adoção de um computador que implemente técnicas de *firewall* para garantir proteção às estações de trabalho e ao servidor, possibilitando maior segurança nas transações de dados. Esse computador desempenharia o papel de um servidor de Internet, tendo implementadas, além de técnicas de *firewall* de pacotes e *proxy*, técnicas de rede privada virtual e controle de navegação da Internet. Sugere-se também a aquisição de servidor adequado às necessidades da rede de computadores. Nesse servidor, podem ser aplicadas técnicas de *firewall*, que irão conferir um nível ainda maior de segurança à informação que trafega na rede interna de computadores.

3.2.2 Antivírus

Dentre os computadores que compõem o parque tecnológico da empresa, somente alguns poucos possuem instalado sistema antivírus. Além disso, mesmo

nas poucas máquinas que tem esse sistema, a varredura em busca de programas maliciosos não é feita rotineiramente.

Sugere-se a utilização de sistema antivírus em todos os computadores, além de sistema antivírus específico para os servidores, caso venham a ser implementados. Além disso, caso seja adotado servidor de Internet, sugere-se ainda liberação de endereços para atualização automática dos sistemas. Também há que se considerar a varredura em busca de programas maliciosos em todas as máquinas, a ser programada para ocorrer fora do horário de trabalho. Dessa forma, as varreduras em busca de programas maliciosos poderão ser executadas sem que haja lentidão nos computadores durante o expediente.

3.2.3 Zona desmilitarizada

Tendo sido sugerido a adoção de um servidor de Internet com serviços de *firewall proxy* e de pacotes e levando-se em consideração que a empresa não disponibiliza arquivos em domínio ou área de acesso público, este estudo não considera necessária a implantação de uma zona desmilitarizada.

3.2.4 Criptografia

O sistema informatizado utilizado na empresa já proporciona cifragem de todos os dados manipulados através dele. Então, este estudo não considera necessária a utilização de criptografia adicional nas comunicações realizadas entre computadores da rede local de computadores.

Os computadores que não estão conectados à rede local da empresa utilizam mídias removíveis para transporte dos dados. Para enviá-los, é gerada remessa de dados que é transportada em uma mídia até a sede da empresa. Então, a remessa de dados é importada, realizando a inserção de dados no banco de dados principal.

Para otimizar a comunicação e conferir maior segurança na comunicação dos dados entre as filiais da empresa e a matriz, sugere-se utilizar o servidor de Internet,

apresentado como necessário no item 3.2.1, para que sejam feitas conexões criptografadas de rede virtual privada, ou ainda sejam disponibilizadas contas de serviços de terminal.

Em uma rede virtual privada, é utilizada a rede pública de computadores (Internet) para estabelecer um canal particular de comunicação. Assim, para conectar duas ou mais redes distantes fisicamente, é criado um canal de comunicação criptografado entre elas. Na comunicação, os dados são cifrados e encapsulados pelo protocolo IP, para serem transmitidos pela Internet. Os dados são novamente encapsulados por outro protocolo utilizado na conexão e, então, os dados são enviados pela rede. Essa solução é economicamente viável, independente da distância física entre as duas redes, em comparação com as alternativas de cabeamento e canais dedicados de comunicação.

Nos serviços de terminal, uma conexão criptografada é estabelecida entre um servidor e a estação de trabalho remota. Os serviços de terminal utilizam protocolo que comprime e cifra automaticamente os dados na conexão, fazendo com que, na maioria das vezes, seja uma solução com melhor desempenho, em relação às redes privadas virtuais.

3.2.5 Certificados

Esta análise, levando em consideração a atual estrutura tecnológica da empresa, não considera necessário a utilização de certificados. No entanto, caso a empresa opte pela utilização de serviços de terminal, a utilização de certificados torna-se interessante por conferir um nível mais elevado de segurança às informações que trafegam pela Internet.

3.2.6 Esteganografia

Este estudo não considera necessária a utilização de técnicas de esteganografia nos processos de comunicação da empresa, a menos que

informações sejam disponibilizadas aos clientes via Internet. Nesse caso, talvez seja interessante utilizar técnicas de esteganografia em marcas d'água nos documentos, além do logotipo da empresa. A utilização dessas técnicas fará com que se torne mais difícil a falsificação de qualquer documento emitido pela empresa.

3.3 Segurança Física

A empresa conta com sistemas de alarme abrangendo todo o terreno onde está localizada. Além disso, é circundada por cercas elétricas. Essas duas medidas dificultam que invasores obtenham acesso às dependências da empresa, fora do expediente de trabalho. Para ter acesso à área interna da empresa durante o expediente, deve-se utilizar um pequeno portão de aço, localizado atrás da recepção da empresa. Porém, esse portão está sempre aberto, permitindo que qualquer pessoa acesse, durante o horário comercial, as dependências da empresa e tenha acesso aos computadores. Portando, existe risco de violação da segurança das informações. Além disso, existem casos relatados de invasões à empresa que resultaram em furtos aos colaboradores.

Sugere-se que o perímetro da empresa seja completamente coberto por circuito fechado de monitoramento de imagens, com câmeras estrategicamente posicionadas. Sugere-se ainda que o portão de aço permaneça fechado, para que somente pessoal autorizado tenha acesso às dependências da empresa. A adoção de um dispositivo de alerta silencioso na recepção da empresa também deve ser considerada.

3.4 Segurança Humana

A empresa não dispõe de programas de qualificação de pessoal quanto ao bom uso dos equipamentos e quanto às práticas de engenharia social. Equipamentos são constantemente danificados ou subutilizados, por não haver pessoal treinado para sua utilização. Além disso, já houve casos de engenharia

social na empresa, quando pessoas mal intencionadas, usando argumentos razoáveis, obtiveram dados e documentos importantes da empresa, o que somente foi percebido mais tarde, quando outras instituições entraram em contato com a empresa a fim de confirmar algumas informações.

Sugere-se o desenvolvimento de um programa de treinamento de todos os funcionários que utilizam os equipamentos de informática ou a adoção de programas de incentivo ao aperfeiçoamento profissional do funcionário, a fim de manter, em seu quadro de recursos humanos, profissionais plenamente capacitados ao desempenho de suas funções. Ainda, sugerem-se treinamentos em técnicas de identificação e resistência aos ataques de engenharia social, a fim de evitar perdas significativas de dados e preservar as informações que estão sob responsabilidade da empresa.

4 CONSIDERAÇÕES FINAIS

Crimes e criminosos sempre existiram e sempre existirão. Crimes digitais também, envolvendo diversos tipos de criminosos com objetivos diferentes. Bruce Schneier (2001) comenta que poderiam ser classificados como *hackers*[3] curiosos, criminosos em busca de ganhos financeiros, *insiders*[4] maliciosos em busca de vingança, ganhos financeiros ou publicidade, espiões em busca de informações vantajosas, entre outros.

Um ambiente completamente seguro, segundo Peixoto (2005), jamais existirá. De acordo com Schneier (2001), o que se pode é conferir aspectos de segurança física, humana e tecnológica, de acordo com a necessidade identificada ou com o valor estimado da informação para a organização.

Informações relativas à saúde de alguém devem estar disponíveis somente às pessoas realmente autorizadas, pois sempre existem criminosos que tentarão obter alguma vantagem utilizando essas informações. Por exemplo, no caso da empresa estudada, as informações ficam sob guarda da empresa, então é responsabilidade dessa conferir tantas características de segurança quantas forem possíveis a nível tecnológico, físico e humano.

Adicionando as características de segurança mencionadas acima às informações do paciente, objetiva-se garantir que essas informações sejam confidenciais, somente podendo ser acessadas por pessoal com tal autorização e necessidade. Além disso, pretende-se garantir que essas informações não sofram alterações duvidosas ou não autorizadas durante o período de tempo em que ficam sob guarda da empresa, além de tornar essas informações disponíveis ao paciente quando necessitar.

Peixoto (2005) cita a necessidade de se pensar na segurança da informação também nos aspectos físico e humano, apesar de a área tecnológica ser a que geralmente recebe mais investimentos. Schneier (2001) cita que, ao invés de afirmar que uma informação está protegida, deve-se citar contra o quê ela está protegida. Além disso, Peixoto (2005) afirma que o fator humano está presente no sucesso ou

[3] Conforme Schneier (2001), a palavra *hacker* possui diversas definições possíveis, desde um administrador de sistemas corporativos eficiente até um criminoso adolescente com pouca ética. A palavra descreve alguém com determinado conjunto de habilidades.
[4] Conforme Schneier (2001), um *insider* é alguém que tem acesso a informações sigilosas.

fracasso da maioria dos episódios que envolvem segurança ou problemas de segurança da informação, devendo esse aspecto da segurança merecer atenção especial.

Dentre as diversas soluções propostas, a empresa procurou adotar aquelas que julgou serem adequadas ao seu ramo de negócio e ao porte da empresa. Nas três áreas abordadas, algumas sugestões foram vistas como importantes para a continuidade do negócio. Segue abaixo a descrição das sugestões, acatadas ou não, e uma imagem de como ficaria a segurança tecnológica da empresa após a implantação dessas sugestões.

Segurança tecnológica

- *Firewall*: foi sugerida a implantação de um servidor de Internet com implementação de técnicas de *firewall* de pacotes e de *proxy.* A empresa julgou a sugestão e considerou ser importante para conferir maior segurança às transações de informação. Além disso, foi sugerida também a implantação de um servidor de banco de dados adequado às necessidades da empresa, também com técnicas de *firewall* implementadas e sistema antivírus. A empresa julgou como importante adotar a solução sugerida. Então, providenciou a aquisição de um servidor adequado, que desempenha a função de servidor de bancos de dados, porém sem sistema antivírus e utilizando as técnicas de *firewall* nativas do sistema operacional. A outra máquina utilizada como servidor de uso geral atualmente é utilizada como servidor de banco de dados dos usuários da rede[5], armazenando e gerenciando dados relativos ao acesso dos usuários à rede de computadores, também sem sistema antivírus e utilizando apenas as técnicas de *firewall* nativas do sistema operacional. Ambos os servidores utilizam sistema operacional Windows Server 2003.

[5] Banco de dados dos usuários da rede: esse banco de dados chama-se “Active Directory”, e é responsável pelo armazenamento de informações e permissões de acesso aos usuários da rede de computadores.

- Antivírus: foi sugerida a adoção de sistemas antivírus nas estações de trabalho, o que foi categorizado pela direção da empresa como sendo uma solução muito importante para conferir um nível mais elevado de segurança aos computadores da rede e às informações que trafegam pela rede. As atualizações dos antivírus são efetuadas quinzenalmente, utilizando o método de atualização manual, conforme decisão do responsável pelo setor.
- Certificados: foi sugerida a adoção de certificados nas comunicações entre a rede de computadores e as estações que utilizam acesso remoto. Porém, como as estações já utilizam acesso com criptografia de dados, a direção da empresa considerou desnecessário adoção de certificados.
- Esteganografia: foi sugerida a utilização de técnicas de esteganografia, caso fossem disponibilizados documentos na Internet. Porém, como a empresa fornece senhas de acesso ao médico assistente e somente envia documentos aos pacientes quando solicitados e com confirmação de dados pessoais do cliente, a empresa julgou desnecessária a adoção de técnicas de esteganografia aos documentos.

Segurança física

- Câmeras de monitoramento: foi sugerida a adoção de câmeras em um circuito fechado de monitoramento de imagens. Porém, como a empresa disponibiliza de um circuito de sensores de movimento, acionados via senhas de acesso, e monitorados por empresa terceirizada de segurança, a empresa julgou desnecessário adotar tal sugestão.
- Restrição à entrada: foi sugerido que o portão de acesso à área interna da empresa permaneça fechado, permitindo o acesso somente às pessoas autorizadas. Tal medida foi acatada e, a partir de então, um funcionário da empresa efetua a seleção das pessoas que podem ou não entrar na empresa. Para sair, um mecanismo próximo ao portão garante a abertura, além de outro mecanismo garantir o fechamento automático do portão.

- Dispositivo de alerta: foi sugerida a adoção de um dispositivo de alerta silencioso na sala de recepção. Tal medida foi considerada como muito interessante pela direção da empresa. Então, o dispositivo foi instalado em alguns pontos da sala de recepção. Quando acionado, um alarme soa, em um setor interno da empresa, demonstrando o perigo e provocando o acionamento policial ou de pessoal capacitado a enfrentar situações de risco.

Segurança humana

- Treinamentos: foi sugerida a adoção de treinamentos para melhor utilização dos equipamentos de informática. Tal sugestão foi acatada pela direção da empresa, sendo promovidos levantamento e padronização de todas as rotinas internas que utilizem computadores. Depois disso, foi efetuado treinamento de todos os usuários.
- Engenharia social: foi sugerido que, além de treinamentos para melhor utilização dos equipamentos, fosse fornecido treinamento para capacitar os funcionários a identificar e a resistir a ataques de engenharia social. Essa sugestão foi acatada pela empresa, que passou a utilizar sistemática de sigilo de todas as informações tratadas no processo produtivo, além de incluir nos treinamentos citados no item anterior uma seção para tratar dos ataques que utilizam engenharia social.
- Incentivos: foi sugerida a adoção de incentivos à qualificação e requalificação profissional. Porém, como a empresa já trabalha com política de incentivos profissionais, a direção não julgou necessário adicionar mais esse tipo de incentivo.

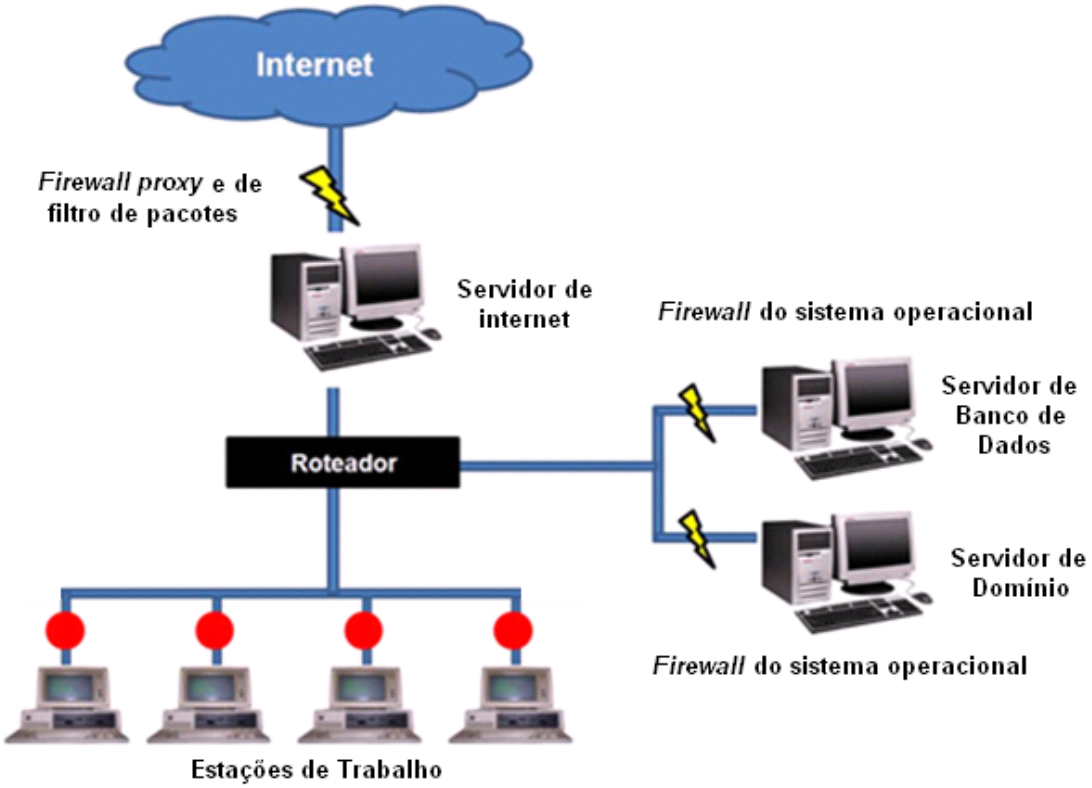

FIGURA 7: Situação da segurança tecnológica na empresa após as sugestões adotadas.
Fonte: Arquivo pessoal.

A Figura 7 ilustra o cenário de segurança da informação na empresa após as sugestões acatadas. Desse modo, pode-se observar a atual situação das informações trabalhadas na empresa. Os detalhes em amarelo representam os pontos em que foram adotadas técnicas de *firewall* e os detalhes em vermelho representam os pontos em que foram adotados sistemas antivírus.

Pôde-se verificar que muitas das sugestões foram acatadas pela empresa a fim de conferir um maior nível de segurança às informações com que trabalha. Como já foi mencionado, um cenário em que as informações estarão completamente seguras é utópico. Então, compete aos responsáveis aumentar o máximo possível a quantidade de características de segurança aplicadas ao negócio e à informação trabalhada, prevenindo ataques e definindo medidas reativas em caso de algum ataque de sucesso.

REFERÊNCIAS

AGREDA, Carlos. **Esteganografia em Imagenes**. 2008. Lima. Disponível em: <http://carlosagreda.blogspot.com/2008/02/esteganografia-en-imagenes.html>. Acesso em: 03 dez. 2008.

ANDRADE, Edson de Oliveira; SILVA, Rubens dos Santos. **RESOLUÇÃO CFM nº 1.638/2002. "Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde"**. Brasília, 2002.

ARAÚJO, Marcelo Yamada. **Conceitos e a Norma ISO 27001 em Sistemas de Gestão de Segurança da Informação**. São Paulo, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799: Tecnologia da informação** - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001. 56p.

BEAL, Adriana. **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BUSTAMANTE, Leonardo. Esteganografia: A Arte de Esconder. **Computação Forense**. 2006. Disponível em: <http://imasters.uol.com.br/artigo/4500/forense/esteganografia_-_a_arte_de_esconder/>. Acesso em: 07 out. 2008.

CAVALCANTI, Elmano Pontes. REVOLUÇÃO DA INFORMAÇÃO: ALGUMAS REFLEXÕES. **Caderno de Pesquisas em Administração**, São Paulo, v.1, n.° 1, 2° semestre/1995. Disponível em: < http://elmanocavalcanti.sites.uol.com.br/epcpa002.htm>. Acesso em: 14 set. 2008.

FERREIRA, Aurélio Buarque de Holanda. **Novo Dicionário Eletrônico Aurélio**. Versão 5.0. Positivo Informática, 2004.

GONÇALVES, Luís Rodrigo de Oliveira. Pequeno histórico sobre o surgimento das Normas de Segurança, 2003. **Módulo Security Magazine**. Disponível em: <http://www. modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=344&pagenumber=0&idiom=0>. Acesso em: 30 mar. 2008.

LAUREANO, Marcos Aurélio Pchek. **Gestão de Segurança da Informação**. 2005. Curitiba. Disponível em: < http://www.mlaureano.org/aulas_material/gst/apostila_versao_20. pdf>. Acesso em: 17 jun. 2008.

PEIXOTO, Mario César Pintaudi. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2005.

PETERSON, Larry L. **Redes de computadores: uma abordagem de sistemas.** Rio de Janeiro: Elsevier, 2004.

PINHEIRO, José Mauricio Santos. **Redes de Perímetro**. 2004. Disponível em: <www.projetoderedes.com.br/artigos/imagens/image25.gif >. Acesso em: 03 dez. 2008.

PIROPO, B. **Atributos Digitais I:** Confidencialidade e autenticação. 2007. Disponível em: <http://www.bpiropo.com.br/graficos/FPC20071203_1.jpg>. Acesso em: 03 dez. 2008.

RAPOPORT, Eduardo. **VPN - Conceitos**. 2003. Rio de Janeiro. Disponível em: <http://www.gta.ufrj.br/~rezende/cursos/eel879/trabalhos/vpn/conceitos_assimetrica.gif>. Acesso em: 03 dez. 2008.

SCHEINKMAN, José Alexandre. A lição de Willie Sutton ao PT. 2006. ***Folha de São Paulo.*** Disponível em < http://www.gabeira.com.br/noticias/noticia.asp?id =2631>. Acesso em: 17 jun. 2008.

SCHNEIER, Bruce. **Segurança.com:** segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001.

SILVA, Alexandre Parra C. da; WESTPHALL, Carla Merkle; WESTPHALL, Carlos Becker. *ChiWa*: Implementação da Segurança Multilateral através do Refinamento da Política Chinese Wall. ***Revista Eletrônica de Iniciação Científica, Publicação da SBC (Sociedade Brasileira de Computação)***, Porto Alegre, v. 3, n. 4, 2003. Disponível em <http://www.sbc.org.br/reic/edicoes/2003e4/>. Acesso em: 19 jun. 2008.

SILVA, Pedro Tavares; CARVALHO, Hugo; TORRES, Catarina Botelho. **Segurança dos Sistemas de Informação**: Gestão Estratégica da Segurança Empresarial. Lisboa: Centro Atlântico, 2003.