Paulo Henrique Coelho Andrade

Segurança de perímetro de rede em conformidade com os padrões NBR ISO/IEC 17799 (BS7799) e C2

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-Graduação Lato Sensu em Administração em Redes Linux, para obtenção do título de Especialista em Redes Linux.

Orientador
Prof. Msc. Sandro Pereira de Melo

LAVRAS
Minas Gerais – Brasil
2007

Paulo Henrique Coelho Andrade

Segurança de perímetro de rede em conformidade com os padrões NBR ISO/IEC 17799 (BS7799) e C2

Monografia apresentada ao Departamento de Ciência da Computação da Universidade Federal de Lavras, como parte das exigências do curso de Pós-Graduação Lato Sensu em Administração em Redes Linux, para obtenção do título de Especialista em Redes Linux.

Aprovada em 31 de Março de 2007

_____

Prof. Msc. Herlon Ayres Camargo

_____

Prof. Dsc. Marluce Rodrigues Pereira

_____

Prof. Msc. Sandro Pereira de Melo (Orientador)

LAVRAS

Minas Gerais – Brasil

2007

DEDICATÓRIA

Dedico este trabalho a minha querida filhinha Giovanna que nasceu no mês que tive a primeira oportunidade de apresentar este trabalho, a qual adiei para a segunda oportunidade, para presenciar seu nascimento. Ela ainda não tem consciência, mas todo o tempo em que dedico estudando e trabalhando é para tentar conquistar uma posição mais confortável e garantir um futuro melhor para ela e também a minha querida esposa.

AGRADECIMENTOS

Gostaria de agradecer a minha esposa, minha mãe e irmã que tiveram muita paciência e compreensão pela horas e horas que estive ausente me dedicando a este trabalho. Também gostaria de agradecer ao meu orientador Sandro Pereira Melo pelas várias sugestões de material que auxiliou no enriquecimento deste meu trabalho de monografia.

RESUMO

É de conhecimento de muitos que a cada dia que se passa está mais difícil manter as informações seguras, sejam elas pessoais ou corporativas. As mais variadas ferramentas de *software* ou *hardware* existentes buscam os mesmos objetivos, equilibrando segurança, riscos e flexibilidade.

E este trabalho de monografia através do estudo de caso do ambiente computacional da empresa URCTML, realizou uma análise do perímetro de rede e com o auxílio das normas e padrões NBR ISO/IEC 17799, BS7799 e C2, apresenta uma análise dos resultados. Propor melhorias e ainda propor uma mudança no *layout* do perímetro de rede.

Ainda neste trabalho, será comentado sobre recursos e ajustes recomendados para se realizar no servidor *firewall.* Estes ajustes são em nível de kernel e na área utilizada pelos usuários, chamada USERSPACE. Por último será apresentado o resultado da análise, caso o objetivo tenha sido alcançado, e serão propostas mudanças.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

BS - *British Standart*

BS7799 - *British Standart 7799*

IEC - *International Engineering Consortium*

ISO - *International Standartization Organization*

NBR – Norma Brasileira

TI – Tecnologia da Informação

EUA – Estados Unidos da América

SOHO - Segmento do mercado composto por empresas de pequeno porte e escritório domésticos

C2 - Nível de segurança definido pelo TCSEC, e exigido pelo Departamento de Defesa dos Estados Unidos

OSI - *Open Systems Interconnection*, Camadas OSI ou Interconexão de Sistemas Abertos, é um conjunto de padrões ISO relativo à comunicação de dados

DTI - *Department Of Trade Centre*

CCSC - Comercial Computer Security Centre

TCSEC - Truster Computer Security Evaluation Criteria, é um documento desenvolvido pela Agencia Nacional de Segurança do Governo dos Estados Unidos

CC – *Common Criteria*, padrão internacional de segurança de computador, atualmente tornou-se a ISO/IEC 15408

NAT - Network Address Translation, também chamado de *masquerade,* consiste na técnica de reescrever os IP´s de origem, passando sobre um *firewall* / roteador à acesso externo

Sumário

1. Introdução

Com o surgimento da rede global, a Internet, houve também uma grande preocupação com as informações devido ao risco de possíveis invasões e a possibilidade destas informações se tornarem acessíveis a qualquer pessoa conectada à Internet ser uma realidade. Para garantir a segurança dessas informações é necessário muito mais do que apenas implementar uma ferramenta ou aplicar uma tecnologia de segurança. As organizações começaram a se preocupar com a segurança da informação e suas premissas, e essas variam de acordo com seus níveis de segurança aplicados no ambiente, seja ele SOHO ou Corporativo e, assim, garantir a qualidade, confidencialidade, integridade e disponibilidade dessas informações.

Para esta garantia, torna-se indispensável que o ambiente possua um firewall, também chamado de parede de fogo ou parede corta fogo, que nada mais é que: “o nome dado ao dispositivo de uma rede de computadores que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede para outra”. No mesmo conceito incluem-se: os filtros de pacotes e os *proxys;* a implementação de um *checklist* pode se transformar no estado da arte em relação a prevenção de problemas para os administradores [10].

O *firewall* é utilizado para evitar que o tráfego não autorizado possa fluir de um domínio de rede para o outro. Apesar de se tratar de um conceito geralmente relacionado à proteção de um sistema de dados contra invasões, o *firewall* não possui capacidade de analisar toda a extensão do protocolo, restringindo-se geralmente ao nível 4 da camada OSI [13], e através de módulos agregados podendo trabalhar em outras camadas OSI. [7]

Neste trabalho de monografia, serão propostas medidas que servirão de auxilio a análise, e serão utilizadas num perímetro de rede que se deseja tornar seguro, usando como base e referência os padrões e normas da ISO/IEC 17799, práticas aplicadas da BS7799 com auxílio de ferramentas do ambiente Linux.

Algo importante a ser lembrado é que cada caso é um caso. Este trabalho servirá de referência comum à muitos ambientes, porém há situações não aplicáveis em determinados ambientes computacionais. É tarefa do administrador de redes avaliar a sua aplicabilidade ou não no ambiente em questão.

Esse trabalho não pretende exaurir os assuntos, mas apresentar uma noção e proposta do caminho a seguir na implementação de segurança em redes. Usou-se como estudo de caso para o levantamento desses requisitos a empresa com pseudônimo de URCTML.

1.1 Motivação

Quando se fala em proteção de um bem ou um ativo de informação, significa que este tem um valor e, que muitas vezes, é imensurável ou irrecuperável. Não se trata apenas de uma segurança física, mas também de uma segurança lógica.

A motivação para a realização deste trabalho, originou-se na ausência de critérios ou políticas de segurança, quando ingressei na empresa que trabalho atualmente. Muitos itens já foram implementados desde então, como treinamento básico aos colaboradores sobre a segurança da informação, um controle de autenticação centralizado, *gateway* de Internet através de regras simples do IPTABLES e filtro de conteúdo com o SQUID-PROXY, sem falar na infra-estrutura e cabeamento estruturado que era inexistente.

É difícil conseguir segurança quando não se adota critérios ou padrões, surgiu-se então, a idéia de propor a adoção de padrões como a NBR ISO/IEC 17799, práticas (BS7799) e nível de segurança C2 definido pela TCSEC e utilizado pelo Departamento de Defesa dos (EUA), no perímetro de rede da empresa URCTML, utilizado como estudo de caso.

1.2 Objetivos

1.2.1 Objetivos Gerais

O objetivo deste trabalho é entender e analisar o perímetro de rede de uma organização, que receberá o nome fictício de URCTML, para preservar sua integridade e imagem. Em posse dos resultados, sugere-se a aplicação de uma política de segurança adequada para a organização, utilizando como referência a norma anteriormente falada.

Sabe-se que há inúmeros fatores que estão envolvidos na segurança de um perímetro de rede, os *softwares* são um dos ativos mais importantes na implementação das normas e ou padrões de segurança, mas não são os únicos, pois questões físicas também devem ser observadas.

1.2.2 Objetivos Específicos

Este trabalho visa sugerir a construção de um ambiente de rede seguro, sabe-se que a norma adotada, a NBR ISO/IEC 17799, dentre os seus capítulos, procura alcançar os mais variados aspectos de uma segurança organizacional, que por ser um assunto bem amplo, não serão considerados em sua íntegra, mas terão o apoio dos recursos conseguidos com o nível de segurança C2, e ajustes em nível de kernel e USERSPACE.

Este trabalho tem como objetivo também, sugerir soluções práticas com o auxilio da BS7799, implementações de políticas de segurança, e que os riscos sejam fortemente diminuídos. Este trabalho, também servirá como incentivo e colaboração, inspirando outros acadêmicos a somar com o mesmo.

1.3 Escopo e Metodologia

Este trabalho de monografia tem como estudo de caso o ambiente da empresa URCTML, e neste será realizado um levantamento de requisitos e análise da situação atual do ambiente. Baseando-se nos resultados desta análise, serão elaboradas várias sugestões e propostas de *hardening* do sistema como um todo. Os trabalhos de levantamento e análise foram realizados a partir do mês de julho até meados de outubro de 2006, durante os horários de folga e fora do expediente de trabalho.

Para melhor organizar a execução do trabalho, o mesmo foi segmentado em três partes, sendo: coleta de informações, análise e sugestões para a melhoria das políticas e práticas de segurança através dos resultados da análise.

Durante a coleta observou-se que algumas políticas e controles já estavam sendo aplicadas no ambiente em estudo. Os questionamentos utilizados para coletar os dados tiveram como referência a documentação [6], mas foram modificados e adaptados pelo autor deste trabalho. Apenas foram considerados os itens da norma de segurança ISO/IEC 17799:2005 pertinentes ao ambiente em estudo. Também no processo de coleta, criou-se um mecanismo próprio de pontuação dos itens.

Na parte de análise, realizou-se a validação das questões levantadas na etapa anterior e realizou-se a pontuação de cada item. Em outra etapa contabilizou-se a pontuação total dos itens e realizou-se sugestões baseadas nos resultados que possam melhorar o controle e aumentar a segurança do ambiente computacional como um todo.

Como o tema deste trabalho é bastante amplo e seu objetivo atual não é a implementação, o mesmo não se aprofundará em questões operacionais sobre como fazer e sim dirá o que deve ser feito, visando manter seus interesses científicos e viabilizando o uso como fonte de pesquisa e referência para outros trabalhos futuros. Os interessados em utilizar este trabalho como fonte de pesquisa e talvez implementação, devem verificar as referências.

1.4 Estado da Arte

A cada dia a segurança da informação se torna o assunto mais falado e discutido dentre os muitos importantes para o administrador de TI. Várias fontes de consulta e ferramentas de *hardware* servem como consulta a referências para a prevenção do sistema de informação. Uma confirmação disso são as novas normas que surgem, como a ISO/IEC 27001, que vêm substituir a norma BS-7799 part2, tratando de Sistemas de Gestão de Segurança da Informação. Sua utilização está diretamente relacionada à ISO/IEC 17799:2005 [10].

A publicação da ISO/IEC 27001:2005 é aguardada há algum tempo ansiosamente pelo mercado, pois trata de questões de proteção das informações, de ameaças e vulnerabilidades, diminuindo riscos, garantindo a continuidade dos negócios, a conformidade aos requisitos legais, regulamentares e ainda preservando a imagem da empresa. Proteção essa a partir de implementações de vários controles como, por exemplo, políticas, procedimentos, recursos de *software* e de *hardware;* englobando pessoas, processos e sistemas de Tecnologia da Informação. A maioria das organizações, independentemente do seu porte ou área de atuação, podem usar como referência a norma ISO IEC 27001:2005 [10].

A publicação desta norma demonstra a importância conquistada pela segurança da informação, sendo percebida até como fator estratégico de negócio à qualquer empresa. Para fornecer suporte a ISO IEC 27001:2005, a equipe da ISO/IEC, criou uma família de normas sobre gestão da segurança da informação, chamada de série 27000. Em novembro de 2006, foram homologadas as seguintes normas e projetos de normas da série 27000:

- ISO IEC NWIP 27000, *Information Security Management Systems - Fundamentals and Vocabulary;*
- ISO IEC 27001:2005, *Information Security Management Systems- Requirements;*
- ISO IEC 27002:2005, *Information Technology – Code of practice for information Security Management;*
- ISO IEC 1 st WD 27003, *Information Security Management Systems- Implementation Guidance;*
- ISO IEC 2nd WD 27004, *Information Security Management- Measurements;*
- ISO IEC 2nd CD 27005, *Information Security Management Systems- Information Security Risk Management.*

1.5 Organização do Trabalho

Este trabalho de conclusão de curso está estruturado e dividido em 6 capítulos, sendo que o capítulo 1, contém uma introdução sobre o trabalho, motivações da pesquisa e proposta de implementação.

No capítulo 2, encontram-se conceitos de um perímetro de rede, exemplificando o perímetro atual da empresa URCTML, usada como estudo de caso e uma sugestão de modificações no perímetro para minimizar suas possíveis vulnerabilidades depois de uma análise crítica, justificando as mesmas.

No capítulo 3, serão apresentados os níveis de segurança, suas subdivisões, recursos utilizados e benefícios adquiridos.

No capítulo 4, é apresentada uma proposta de *hardening* do *kernel*, que se trata de uma customização e otimização do k*ernel* através de ajustes de segurança, recursos utilizados e benefícios adquiridos com a aplicação do *patch* LIDS e algumas alternativas a ele com *PAX* e *SELINUX*.

No capítulo 5, encontram-se algumas considerações sobre as políticas de segurança implementadas, compatibilizando-as com os requisitos, apresentando a análise e os resultados conseguidos com sua implementação.

No capítulos 6, são realizadas algumas considerações finais sobre o trabalho e uma análise conclusiva do mesmo.

2. Perímetro de Rede

2.1 Fundamentação Teórica

A origem da ISO/IEC 17799 ocorreu no final da década de 80. Em 1987, no Reino Unido, o DTI criou o CCSC para auxiliar as companhias britânicas que comercializavam produtos, e precisavam de critérios para avaliação da segurança [10].

Em 1995, esse código foi revisado e publicado como uma norma britânica BS, a BS7799:1995. A versão aplicada em países de língua portuguesa é a NBR ISO/IEC 17799 [10].

As práticas BS7799 e a Norma ISO/IEC 17799, têm como objetivo fornecer recomendações para a gestão da segurança da informação, fornecer padrões para desenvolvimento de normas e práticas, como também um relacionamento confiável entre organizações [13].

As práticas BS7799 estão segmentadas em três partes: BS7799 parte 1, BS7799 parte 2 e BS7799 parte 3. A BS7799 parte 1 é um padrão publicado pelo BSI em 1995 que após várias revisões fora adotado pela ISO/IEC 17799, práticas para o gerenciamento de segurança da informação em 2000, revisada em junho de 2005 e em 2007 espera-se ser rebatizada de ISO/IEC 27002. A BS7799 parte 2, fora publicada primeiramente em 1999 pelo BSI, onde são definidas todas as especificações necessárias para um sistema de gerenciamento de estrutura e controle da segurança da informação, padrões de qualidade ISO 9000 e adaptada pela ISO/IEC 27001 em novembro de 2005. A BS7799 parte 3, fora publicada em 2005 atuando na análise e gerência de riscos, comparada a ISO/IEC 27001 [13].

O nível C2 de segurança apresenta um controle maior que o nível anterior (C1), prevendo auditoria das ações independentes de cada usuário do sistema através do processo de *login*. A classe C2 é um nível de segurança mínimo estabelecido para uso pelo Departamento de Defesa dos Estados Unidos. O nível C2 tem como requisito a proteção de acesso controlado. Somente usuários autorizados têm acesso ao sistema e as operações do mesmo, somente são realizadas em modo protegido [8], [9].

O CC fora um resultado de esforços da União Européia, EUA e Canadá em criar critérios comuns a serem utilizados de maneira globalizada. Esse passou por vários ajustes, desde 1996, e só então em 1999, quando sua segunda versão fora homologada, passou a ser chamado e publicado como a norma ISO 15408 [5].

2.2 Conceituação

O perímetro é uma área delimitada por recursos físicos e ou lógicos. Tem como objetivo impedir acesso não autorizado e manter a integridade das

informações da organização.

O nível de proteção deve ser fornecido de forma a compatibilizar com os riscos identificados na análise do mesmo [13].

Para conseguir um ambiente seguro, deve-se levar em consideração, tanto aspectos comportamentais e culturais das pessoas, políticas, normas e procedimentos internos, quanto características físicas do local, sem se esquecer de agentes externos ao perímetro [10].

2.3 Layout do Perímetro da Empresa URCTML

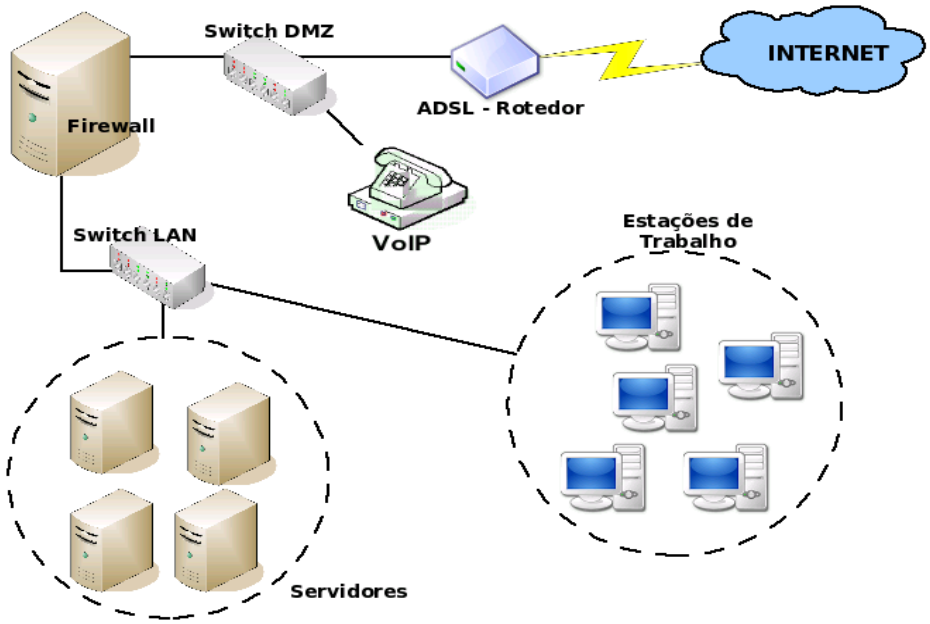

Figura 1: Layout Atual do Perímetro de Rede da Empresa URCTML

A figura 1 não há uma referência literária, é um desenho criado como base na topologia e *layout* de rede atualmente utilizada na empresa URCTML. A figura demonstra como é realizada a interconexão dos ativos da rede, como o serviço de Internet é recebido através de um modem e está conectado a um *switch* que, concomitantemente, liga a um sistema de *VoIP* e ao *firewall*. No *firewall* há uma segunda placa de rede que é conectada a outro *switch* que distribui o sinal de Internet às demais estações da rede.

2.3.1 Análise Crítica

Observa-se no *layout* do perímetro atual da rede da empresa URCTML que existe apenas uma barreira que exerce a função de ponte entre a rede interna da empresa e o meio externo, a Internet. Nesta situação, a empresa torna-se muito exposta, tendo seus riscos aumentados de um possível acesso não autorizado à sua rede local.

O *firewall* implementado neste *layout* tem como função básica funcionar como *gateway* das máquinas da rede, e possui regras simplórias de segurança através do IPTABLES.

Então, uma vez que o possível invasor passe por este *firewall*, não haverá nenhum obstáculo que o impedirá de ter acesso e ou manipular as informações da empresa, quebrando aspectos de segurança como confidencialidade e integridade dos dados.

A figura 2 é um desenho criado com base na topologia e *layout* de rede da empresa URCTML, mas com modificações físicas objetivando melhorar a segurança das informações críticas da empresa em conformidade com as práticas BS7799 [4]. A figura 2 demonstra as modificações realizadas na interconexão dos ativos da rede.

O serviço de Internet é recebido através de um modem e que está conectado a um *switch* ligado a um sistema de *VoIP* e ao *firewall* de fronteira, que tem o objetivo de ser o primeiro obstáculo [4].

No *firewall* de fronteira há duas outras placas de rede que se conectam a outros dois *switchs, um* distribui o sinal de acesso a Internet à um pequeno grupo de estações isoladas da rede de produção; E outra placa de rede distribui sinal as estações de trabalho e se conecta ao *firewall* departamental que serve como segundo obstáculo às informações críticas da empresa, os servidores [4].

2.4 Layout Sugerido para a Empresa URCTML

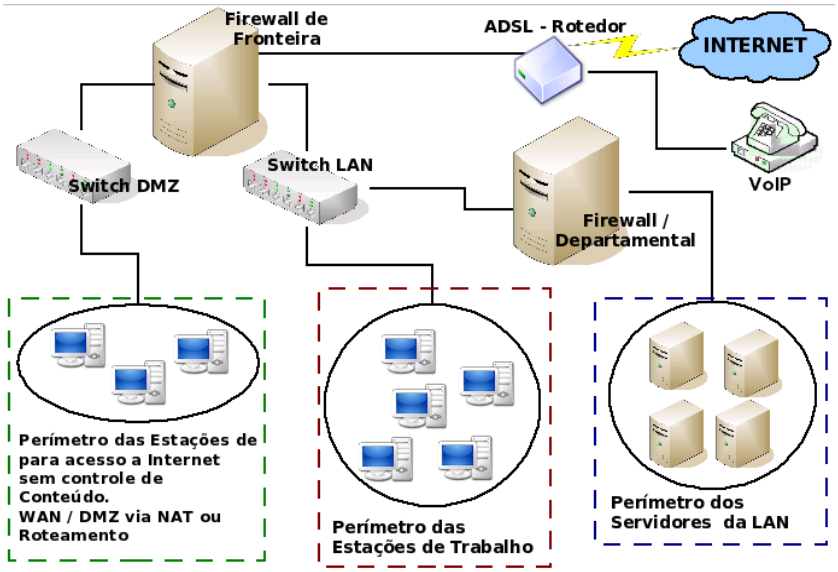

Figura 2: Layout Sugerido do Perímetro de Rede da Empresa URCTML

2.4.1 Justificativa e Conclusão

As mudanças sugeridas no *layout* são para proporcionar um aumento significativo na segurança do perímetro da rede. Foi adicionado um outro *firewall* nomeado como f*irewall* departamental, que tem como objetivo o isolamento das informações críticas da empresa que ficam concentradas nos servidores, e somente a rede local terá acesso, salvo por alguma transação remota que fora explicitamente permitida através do *firewall* de fronteira.

As estações serão segmentadas para também aumentar a segurança do que é trafegado entre a rede local e a Internet. Um dos segmentos terá acesso a Internet, mas com restrições impostas por um filtro de controle de conteúdo a ser acessado. Os demais terão acesso sem controle de conteúdo, mas estarão protegidos pelo *firewall, que estará* analisando as comunicações por trás de regras de roteamento ou NAT, não deixando exposta a identidade do *host* que solicitou a requisição.

As mudanças do *layout*, juntamente com as implementações de normas, políticas e níveis de segurança, aumentarão sensivelmente a segurança do perímetro, fornecendo uma tranquilidade maior ao administrador de redes e à empresa.

3. Níveis de Segurança

3.1 Conceituação

Em 1983, o Departamento de Defesa dos EUA publicou os critérios para avaliação de segurança dos sistemas, o TCSEC (*Trusted Computer Security Evaluation Criteria*), também chamado de "Orange Book" ou "Livro Laranja", por causa de sua capa de cor laranja. Na mesma década alguns países da Europa criaram uma versão de padrão de segurança, nomeado como ITESEC (*Information Techonology Security Evaluation Criteria*), que mais tarde foi renomeada para ITESEM (*IT Security Evaluation Manual*), especificando a mesma metodologia do ITESEC [2].

Quanto aos níveis, o TCSEC define e classifica quatro divisões de proteção, representadas pelas letras, D, C, B e A, sendo a letra "D", a mínima proteção e a letra "A", a máxima proteção [8], [9].

O documento fora elaborado com base em três principais objetivos:

- Proporcionar e incorporar aos produtos dos fabricantes, aspectos de segurança padronizados, incentivando assim a produção em larga escala.
- Fornecer aos membros do Departamento de Defesa dos EUA, formas de se mensurar a confidencialidade no processamento de informações julgadas como sensíveis.
- Fornecer subsídios para que sejam definidas premissas de segurança nas características de compra de equipamentos.

Segundo o TCSEC, um sistema para ser considerado seguro, deve

possuir um controle de seus processos de leitura, escrita, criação e deleção, e somente usuários devidamente autorizados devem ter acesso ao sistema [2].

O Nível de Segurança D, engloba sistemas que têm como características, o mínimo de segurança, e não se encaixem em nenhum outro nível. Os microcomputadores que possuem o sistema baseado em DOS, são exemplos deste nível [2].

O Nível de Segurança C, fornece uma proteção arbitrária em nível de objetos. Por exemplo: (arquivos, diretórios, dispositivos, entre outros), mecanismos onde são atribuídas as permissões a usuários ou grupo de usuários. Este nível é subdividido em duas classes, C1 e C2 [9].

A classe C1, possui proteção com segurança arbitrária, com mecanismos que possam impor limites e impeçam o livre acesso dos usuários, através de identificação dos mesmos. A classe C2, fornece proteção com controle de acesso, com um ajuste mais detalhado em relação à classe C1. Através de autenticação dos usuários, são registrados todos os eventos que posteriormente poderão ser auditados. Também são restringidos acessos à área privada da memória [2].

O nível de segurança B, é uma segurança obrigatória para objetos TCB (*Trusted Computing Base)*, e um conjunto de mecanismos e parte do sistema, incluindo, *hardware, software* e *firmware*, responsável em fornecer e aplicar proteção ao meio computacional. Tem como principal objetivo garantir a integridade dos rótulos de controle que são associados a cada objeto. O nível B é subdividido em três classes: B1, B2 e B3 [2].

A classe B1, engloba todas as premissas da classe C2 e mais outros mecanismos de controle de segurança, como: vinculação de rótulos de segurança aos dados e um mecanismo de controle de acesso obrigatório.

A classe B2, possui as características da B1, e obedece ao modelo formal de TCB, possuindo mecanismos que impõem controle de acesso arbitrário e obrigatório ampliado a todos os usuários e objetos do sistema computacional, mantendo a integridade do sistema durante sua operação.

A classe B3, reúne as características das classes anteriores, e é capaz de operar como monitor de referência, onde todos os acessos dos usuários e objetos do sistema são intermediados, e imune à adulterações. O TCB é bem simples, mantendo apenas códigos essenciais para implementação das políticas de segurança e é um mecanismo de auditoria avançado e capaz de alertar ocorrências de eventos suspeitos possuindo procedimentos de recuperação do sistema, caso ocorra alguma violação [2].

Funcionalmente, o Nível de Segurança A, é equivalente aos sistemas da classe B3, o que diferencia os dois é a análise baseada em técnicas de verificação e especificações formais do projeto do sistema, atribuindo assim à TCB a garantia que a mesma fora implementada corretamente [2].

	Classes de Proteção						
Requisitos	***D***	***C1***	***C2***	***B1***	***B2***	***B3***	***A1***
Auditoria			N	C e	A	A	=
Gerenciamento de Configuração					N	=	C e
Análise de Canais Secretos					N	C	A
Documentação do Projeto		N	=	A	C e	A	C e
Verificação e Especificação do				N	C e	A	C e
Rótulos nos Dispositivos					N	=	=
Controle de Acesso Arbitrário		N	C e	=	=	C e A	=
Exportação de Informação				N	=	=	=
Multiníveis				N	=	=	=
Exportação para Dispositivos com				N	=	=	=
Identificação e Autenticação		N	A	C	=	=	=
Integridade dos Rótulos				N	=	=	=
Rotulação de Saída Legível				N	=	=	=
Rótulos				N	C	=	=
Controle de Acesso Obrigatório				N	C	=	=
Reutilização de Objetos			N	=	=	=	=
Guia do Usuário dos Recursos de		N	=	=	=	=	=

	Classes de Proteção						
Teste de Segurança		N	A	N	C e	C e A	C e
Rótulo de Segurança nos					N	=	=
Arquitetura do Sistema		N	A	A	N	A	=
Integridade do Sistema		N	=	=	=	=	=
Documentação para Testes		N	=	=	A	=	A
Distribuição Segura							N
Recurso de Gerenciamento					N	A	=
Manual dos Recursos de		N	A	A	A	A	=
Rota Segura					N	C	=
Recuperação Segura						N	=

Tabela1: Relacionamento dos requisitos com as classes de proteção do Livro Laranja. [14, pag 479]

A classificação resumida de cada classe está na tabela, na qual associa-se cada serviço exigido à cada classe. Nesta tabela, considera-se o seguinte:

- Um espaço em branco indica que o requisito não é necessário na respectiva classe.
- A letra **A** indica que o requisito não é necessário em classes com nível de proteção inferior e é adicionado à classe referida.
- O símbolo **=** indica que o requisito na classe em questão é igual ao exigido na classe com nível de proteção inferior.
- A letra **N** indica que uma nova definição substitui a definição feita em uma classe inferior.
- A letra **C** indica que o requisito aparece em classe com nível de proteção inferior, porém é modificado na classe em questão [2].

A tabela 1 demostra a classificação das classes de proteção ou como os níveis de segurança agem em cada um dos requisitos de segurança da informação. O relacionamento é feito para melhor explicar qual classe de segurança compreende um determinado requisito.

A missão do Administrador de Redes ou Analista de Segurança é definir

o nível de segurança que será aplicado em determinado perímetro da rede. É importante destacar que quanto mais se fechar a segurança, mais insensível se tornará o ambiente, causando assim, uma certa irritabilidade e impacto aos funcionários.

O profissional de segurança deve buscar no funcionário um aliado, convencendo e afirmando que ele é uma peça importante no processo de implementação de uma política de segurança, independente do nível. Além disso, deve ter sempre o negócio e a missão da empresa como o foco principal [1].

3.2 Recursos Utilizados

Neste trabalho utilizou-se como referência a norma NBR ISO/IEC 17799, as práticas para a gestão de segurança da informação BS7799, e o nível de segurança C2, buscando proteção arbitrária que permita o controle mais rígido dos recursos do sistema, através de autenticação, registro de *log* e auditoria.

Estão agregados ao nível C2 a proteção com segurança arbitrária da classe C1 e a disponibilização de mecanismos que impeçam o acesso livre dos usuários aos recursos do sistema, com possível identificação de cada usuário ou grupo.

Outro recurso utilizado para criar o ambiente com o nível de segurança proposto, é o LIDS (*Linux Intrusion Detection System*). Este recurso é um *patch* de segurança no nível de kernel, que tem como objetivo capacitar o sistema com uma segurança do tipo MAC (*Mandatory Access Control*).

O LIDS transforma a maneira como o sistema funciona, até mesmo o usuário *root*, com todos os seus poderes, estará limitado. Todas as chamadas de sistema serão interceptadas e gerenciadas pelo LIDS [12].

Figura3: Visão do Sistema sem o LIDS. [36, pag 1]

Para exemplificar um sistema sem o uso do LIDS, considere a figura 3, que mostra uma visão macro do funcionamento do sistema. Todas as chamadas de sistema realizadas na área de atuação do usuário são encaminhadas para o kernel, considerando somente o ID do usuário para identificar e classificar se este tem o direito de executar tal chamada [12].

Figura4: Visão do Sistema com o LIDS. [36, pag 2]

A figura 4 exemplifica um sistema com o LIDS. Assim quando o LIDS é configurado, é acrescido ao sistema uma camada que serve para gerenciar todas as chamadas do sistema, permitindo o acesso ao espaço do kernel apenas às chamadas que tenham sido previamente permitidas a partir de uma política de

uso, "*capabilities*".

Após a implementação do LIDS, todos os aplicativos para serem executados deverão ter suas *capabilities* definidas, caso contrário não irão funcionar [12].

3.3 Benefícios Adquiridos

A implementação destes recursos não prova ou garante que uma organização esteja 100% segura. Mesmo que todas as atividades parassem, não há como garantir uma segurança completa. Entretanto, adotando-se certos padrões, normas e níveis de segurança, conquista-se certas vantagens.

As políticas de segurança em uma organização servem para garantir o compromisso e os esforços em busca da segurança da mesma. No meio operacional e de relação humana, obtém-se um melhor conhecimento das fraquezas do sistema, bem como a melhor maneira de protegê-lo, melhorando a consciência dos colaboradores em relação à segurança dentro da empresa.

Outros benefícios em relação à segurança do sistema é um maior controle de todas as atividades que são executadas, independente do autor ou do serviço solicitado de chamada à este, diminuindo, assim as brechas na segurança do mesmo [1].

4. Proposta de *Hardening* para um Servidor *Firewall*

4.1 Conceituação

Hardening nada mais são do que procedimentos de segurança, ou técnicas para ajustes personalizados em um sistema. Estes procedimentos têm como principal objetivo aumentar a segurança do sistema.

Quando as técnicas de *hardening* são aplicadas, existem três fatores que devem ser considerados: segurança, risco e flexibilidade, assim equilibrando-os para melhor manter a continuidade do negócio e com segurança. Não existem sistemas 100% seguros, porém quanto maior a segurança, menor será o risco e

flexibilidade, e, quanto maior a flexibilidade, maior o risco e menor a segurança.

Deve-se entender que não há uma regra, para equilíbrio destes fatores, cada caso deve ser analisado como único, e nem todas as normas e técnicas precisarão ser implementadas [4].

4.1.1 Recursos Utilizados

Como foi comentado anteriormente, nem todas as normas e técnicas têm a necessidade de serem aplicadas. Neste item serão propostas e comentadas algumas técnicas.

- Segurança no Sistema de Arquivos: quando instalamos um sistema Linux, as boas práticas nos recomendam que os principais diretórios sejam particionados separadamente, conseqüentemente, com sua tabela separada. Este procedimento também minimiza uma possível perda de dados caso seja necessário uma reinstalação do sistema.

  Essa não é a única vantagem encontrada, a segurança de um particionamento envolve muito mais do que apenas sua separação. As partições são montadas em diferentes diretórios e diferentes discos rígidos. Para conseguirmos melhorar a segurança destes pontos, pode-se utilizar o comando *mount* que possui uma flexibilidade enorme no que tange à restrições.

  Para estar em conformidade com o item 10.4 da NBR ISO/IEC 17799:2005 [3], é necessário garantir a integridade do *software* e da informação, e a CIS SECURITY também recomenda o controle na utilização do comando *mount*. As sintaxes e exemplos do comando *mount* podem ser encontrados em sua *manpage* e na referência deste [4].

- Utilização de Quotas: através deste recurso é possível um melhor gerenciamento na utilização do sistema de arquivos de todos os usuários do sistema, impedindo assim que quaisquer usuários ou grupo de

usuários ultrapassem os limites físicos de armazenamento dos dados, e facilitando a mensura do *backup* a ser feito.

As quotas devem ser definidas nas partições e não nos diretórios, e configuradas no /etc/fstab (sistema de arquivos montados) [4].

- Remoção de Programas (pacotes) Desnecessários: mesmo com uma instalação básica de um sistema Linux, há inúmeros programas que devem ser removidos, principalmente programas "**clientes**". Este procedimento apesar de ser árduo, é muito importante e está em conformidade com o item 11.5.4 da NBR ISO/IEC 17799:2005 [3], e a CIS SECURITY também cita que tais programas desnecessários podem ser usados para explorar as vulnerabilidades do sistema [4].

- Arquivos com Permissão de *Suid bit*: Este recurso é muito útil, pois é possível definir que determinados binários (executáveis), somente possam ser executados por determinados usuários, que geralmente é o root, administrador do sistema. Os binários que possuem necessidade de remoção das permissões *Suid bit* poderão divergir de um ambiente para outro, portanto recomenda-se uma análise prévia. Em conformidade com o item 11.6.1 da NBR ISO/IEC 17799:2005 [3], o acesso às informações e funções do sistema, deve ser aplicado de acordo com o controle de acesso [4].

- Segurança no Terminal: quando falamos da segurança no terminal, deve-se considerar que a segurança deve ser externa e interna, de nada adianta termos uma ótima segurança de acessos externos, se não há um controle eficaz de acesso no perímetro interno da rede. Em conformidade com os itens 11.5.5 e 11.5.6 da NBR ISO/IEC 17799:2005 [3], um controle de acesso é necessário para que se evite acesso não-autorizado ao sistema [4].

- Gerenciamento de Privilégios: tem como objetivo evitar que o usuário *root* do sistema (usuário administrador), tenha acesso diretamente a um terminal do sistema, facilitando o controle do sistema. Para a execução

de funções do sistema o administrador irá acessar como um usuário comum e posteriormente se tornar *root*. Em conformidade com o item 11.2.2 da NBR ISO/IEC 17799:2005 [3], deve-se estabelecer permissões e uso de privilégios restritos e controlados [4].

- Políticas de Utilização de Serviços de Rede e Serviços Ativos no Sistema: em uma rede de computadores, as práticas de transferir e compartilhar recursos podem proporcionar um ambiente propício para vulnerabilidades e falhas se usadas por usuários mau intencionados. Este procedimento visa restringir o uso destes recursos à usuários que não necessitem do mesmo. Em conformidade com os itens 11.4.2, 11.4.4 e 11.4.6 da NBR ISO/IEC 17799:2005 [3], o usuário só deverá receber o privilégio explicitamente autorizado, utilizar controle de acesso lógico e físico dos serviços e portas [4].

4.1.2 Benefícios Adquiridos

A segurança de um sistema deve partir sempre de uma base de qualidade, que são os pontos de montagem das partições. Com regras simples, é possível conquistar melhor segurança e desempenho do ambiente computacional [4].

Agregado à base de qualidade, pode-se aplicar o sistema de quotas, como uma forma eficiente de se ter o controle quantitativo do que se é armazenado nos pontos montados, ou seja, nas partições [4].

A remoção de programas desnecessários é importante, pois a cada dia que passa, são descobertas falhas e ou brechas nos mais variados programas. Mesmo que se instale um sistema operacional *Linux* com configuração mínima, sempre haverá programas que não serão utilizados pelo administrador ou pelo próprio sistema instalado, e estes podem passar desapercebidos pelo procedimento de *checklist* e *update* do sistema, efetuado regularmente pelo administrador.

Consequentemente, possíveis falhas e ou brechas poderão ser

exploradas por pessoas mau intencionadas, comprometendo a confiabilidade, integridade e até mesmo a disponibilidade do sistema [4].

No sistema *Linux* existem vários arquivos binários, ou seja, executáveis que por padrão possuem permissão de *Suid bit.* Isto quer dizer que são binários possíveis de ser executados por vários usuários do sistema, e desta forma, podem ser usados de forma maléfica, proporcionando uma brecha na segurança. Apenas os binários que realmente podem e devem ser utilizados por outros usuários ou pelo sistema, devem possuir esta permissão, do contrário, a mesma deve ser revogada [4].

A segurança no terminal é importante, pois aumenta a proteção das conexões remotas e evita possíveis ataques. Com simplórias medidas pode-se conseguir ótima proteção ao servidor [4].

Os privilégios do sistema também devem ser bem aplicados a todos os usuários, inclusive ao *root.* Há situações em que mesmo o administrador deve ter limites. Uma ferramenta que pode auxiliar bastante o gerenciamento de privilégios no sistema é o PAM (p*luggable authentication modules, mecanismo* que integra múltiplos níveis de autenticação*). P*ara mais detalhes de sua aplicação consulte seu *manpage* [4].

Outro limite que deve ser imposto no sistema é quanto o acesso aos serviços de rede que estão ativos. Através deles, um *cracker* pode copiar, mover ou até mesmo compartilhar recursos com outros sistemas ou *hosts*. Aplicando limitações em tais recursos, aumentamos a segurança em nosso sistema e diminuímos as chances de um *cracker* encontrar uma brecha no sistema [4].

Todas estas medidas são importantes quando se deseja obter sistemas seguros. Cada uma das medidas adotadas agregam e complementam umas às outras, cada uma em seu nível, mas nem sempre são aplicáveis em todos os casos. Por isso, deve-se sempre dosar as três premissas: segurança, risco e flexibilidade. Ao administrador cabe a missão de realizar uma análise antes da implementação. Porém, a prevenção é a melhor medida a ser adotada [4].

4.2 Tuning do Kernel

4.2.1 Conceituação

O tuning do kernel é a realização de ajustes detalhados, finos ao sistema operacional Linux. Nesta proposta, o objetivo é que estas modificações capacitem o sistema a trabalhar melhor como um firewall, e possibilitando-as ser modificadas em tempo de execução. A manipulação pode ser feita através do sistema de arquivo */proc* ou então através da ferramenta *sysctl,* que está disponível a partir da versão 2.4 do kernel.

Como o objetivo é melhorar a segurança, o desempenho do servidor *firewall* e o tratamento dos pacotes da pilha TCP/IP, deve-se focar três pontos: *tuning* TCP, *tuning* ICMP e *tuning* IP [4].

O protocolo TCP possui características que devem ser lembradas. Os 20 bytes que fazem parte do cabeçalho são importantes para um *firewall,* podendo ser verificado o estado de uma conexão. Estas informações auxiliam na defesa de possíveis ataques [4].

O ICMP é o controle de mensagens do protocolo da Internet, um motivo para o *tuning* ICMP, é que o pacote IP que carrega a mensagem ICMP pode conter informações que podem ser utilizadas com o objetivo de realizar o *fingerprint*, técnicas de extração de informações de um *host* ou alvo. As políticas do *firewall* devem ser equilibradas quanto às solicitações de ICMP do tipo 8 (*echo request*), pois os administradores de rede utilizam com freqüência o ping como ferramenta de diagnóstico. Em um *firewall*, o *tuning* de IP define de as interfaces de rede poderão ou não trocar pacotes entre si.

4.2.2 Segurança do Kernel

O protocolo TCP tem características peculiares. Parte das informações que compõem o cabeçalho dos pacotes deve ser protegida pelo *firewall*, minimizando riscos com ataques de DoS (negação de serviço) e IP *Spoofing*

(falsificação de cabeçalho de IP). O kernel do Linux possui recursos capazes de modificar algumas opções no estado da conexão [4].

Através do protocolo ICMP várias ferramentas são capazes de efetuar diagnósticos em redes. O administrador deve dosar bem sua utilização, pois sua negação completa dificulta o trabalho do administrador. Recomenda-se a liberação de respostas controladas das mensagens do protocolo [4].

Ajustes feitos no protocolo IP são muito importantes, como IP_FORWARD, que bloqueia ou libera o encaminhamento de pacotes entre as interfaces de rede: o RP_FILTER, que auxilia na identificação dos pacotes de origem e evita ataques de IP_SPOOFING. Enfim, o trabalho para ajustes de segurança do kernel em um servidor destinado a trabalhar como *firewall* é importante [4].

4.2.3 Aplicação do patch LIDS

O *LIDS* é um *patch* de *kernel*, portanto está diretamente associado à versão do *kernel* instalado no sistema. Assim, a versão do *LIDS* que for implementada deverá ser correspondente à versão do *kernel* da distribuição *Linux* que está sendo utilizada [12].

Dentre suas características estão: uma boa segurança em nível de kernel e uma configuração robusta. O LIDS funciona entre a USERLAND (*porção da memória do sistema onde são executadas as aplicações dos usuários*) e a KERNELSPACE (*porção da memória do sistema onde são executadas as funções em nível de kernel*), interceptando as chamadas dos usuários do sistema, até mesmo do *root* que se torna um usuário comum, e de acordo com as regras "*compabilities*" definidas, são encaminhadas ou não ao KERNELSPACE, aumentando o controle e a segurança do sistema.

Além da proteção, o administrador pode ser avisado via *e-mail* quando o sistema sofrer alguma alteração ou tentativa de burla ao sistema [4].

Dentre os recursos e benefícios do LIDS podemos citar:

- *Mandatory Access Controls* (MACs), todos os pedidos para acesso a recursos do sistema são submetidos aos controles de acesso, até mesmo o super usuário "root", obedece tais regras estabelecidas.
- Detecção de *Port Scanners:* consegue-se minimizar a ação de scanners à busca de falhas ou vulnerabilidades na rede.
- Proteção de acesso a arquivos e pastas (incluindo o root): torna o sistema bastante flexível, podendo-se definir permissões diferentes para pastas diferentes. As pastas críticas de configuração do sistema podem ter permissão somente leitura e as outras permissões também, como gravação e modificação, execução, deleção.

4.2.4 Alternativas de Segurança

Já foi visto que a ferramenta *LIDS* é indispensável ao administrador de sistemas *Linux*, por proporcionar uma segurança extra e significativa. Além do *LIDS* há outras ferramentas no mercado que também cumprem seu papel de forma semelhante, mas cada uma com suas peculiaridades.

PAX é também um *patch* para o kernel do Linux, que implementa muitas mudanças no sistema, proporcionando-o maior segurança e estabilidade. O *PAX* traz uma proposta extremamente eficiente quando se fala de problemas de vulnerabilidades de alocação de memória no *Linux:* os *buffer overflows* e outras variantes que buscam explorações que dêem ao atacante permissões de leitura e escrita em determinadas áreas da memória do *address space* [15].

O *PAX* funciona de modo a prevenir execuções arbitrárias de códigos para alocação de memória não permitida no sistema. O *PAX* se utiliza de três níveis distintos para determinadas técnicas de exploração: introdução e execução de códigos arbitrários, execução de códigos fora da ordem original do programa, execução de códigos dentro da ordem original do programa usando dados arbitrários. Uma das principais mudanças que o *PAX* causa no sistema é a randomização do *buffer* de saída: o *return address* [15].

O SELINUX (*Security-Enhanced Linux*) [13] é uma implementação de uma flexível e refinada arquitetura MAC (*Mandatory Access Control*). SELINUX provê uma política de segurança sobre todos os processos e objetos do sistema baseando suas decisões em *labels* contendo uma variedade de informações relevantes à segurança. A lógica da política de tomada de decisões é encapsulada dentro de um simples componente conhecido como servidor de segurança (*security server*) com uma interface geral de segurança [13].

SELINUX é parte integrante de algumas distribuições Linux como o Fedora Core e a Red Hat Enterprise Linux [13]. A principal característica é a limitação das ações dos usuários e programas aplicando políticas de segurança em todo o sistema. Quando o sistema não está implementado com o SELINUX, alguns erros de *software* ou alterações de configuração podem tornar o sistema mais suscetível a falhas e ou vulnerabilidades. Assim, as políticas do SELINUX fornecem segurança extra contra o acesso não autorizado [13].

5. Políticas de Segurança

5.1 Considerações

Quando fala-se em Políticas de Segurança, deve-se ter em mente primeiro o conceito de segurança da informação e o que se pretende com as mesmas. Segurança da Informação tem como objetivo proteger os usuários, as informações, o negocio em si, sem esquecer-se de manter a disponibilidade do serviço.

As etapas de uma implementação de Segurança da Informação podem ser resumidas em: Política, Normas, Padrões e Procedimentos. Estas etapas estão interligadas de forma hierárquica [1], [11].

Como pode ser observado na figura 5, é realizada uma interligação entre as três etapas da implantação de segurança da informação e as áreas de atuação dentro da empresa. A área estratégica define todos os ativos que devem estar seguros na empresa e também as políticas de segurança que serão

necessárias para essa proteção [1], [11].

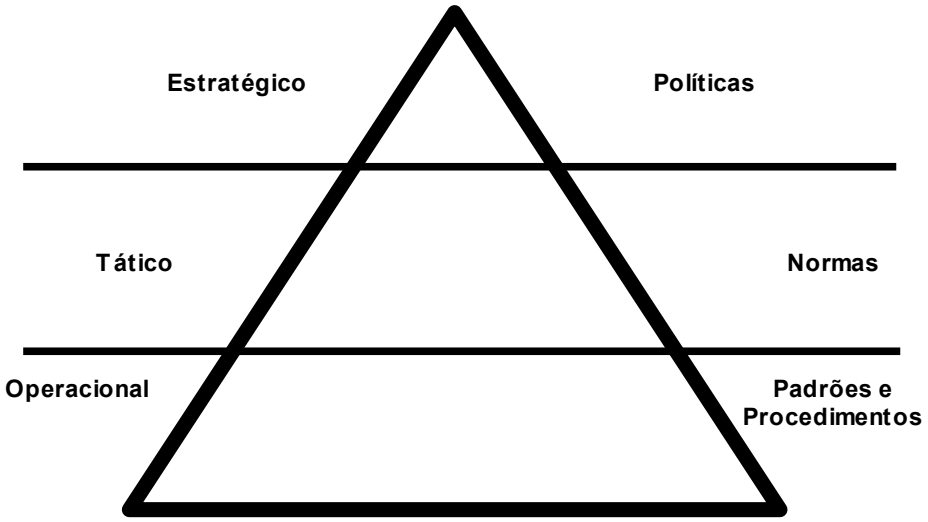

Figura5: Etapas da Segurança da Informação representa por uma pirâmide [4, pag 2]

A parte tática tem a responsabilidade de definir o que deverá ser feito, para garantir que as políticas definidas sejam eficientes e a parte operacional refere-se à aplicação das políticas e táticas definidas [1], [11].

Antes de se definir quais Políticas de Segurança serão utilizadas, deve-se realizar uma análise e fazer as perguntas: O que se espera alcançar? Quais ativos pretende-se proteger? Onde estão localizadas as informações da empresa?

Obtendo as respostas, deve-se avaliar e definir quem deverá ter permissão de acesso aos servidores ou às informações neles contidos. Outro tópico que deverá ser definido é em relação ao nível de segurança, mas sempre focando no negócio da empresa, antes de se definir esses parâmetros. Pois quanto mais limitado for o acesso, mais insensível se tornará o ambiente, causando insatisfações aos usuários [1].

O usuário deve ser envolvido no processo de implantação das Políticas

de Segurança. Esse envolvimento pode ser através da realização de treinamentos, palestras, enfim demostrando os riscos que a empresa e suas informações estão correndo, e quais são as técnicas que podem ser utilizadas para minimizar esses riscos. É também importante mostrar a relevância destas mudanças bem como essas podem contribuir para o crescimento e amadurecimento da empresa [1].

5.2 Conformidade com Requisitos

Um bom ponto de partida para a implementação de segurança da informação é a definição de quais controles serão implementados dentre os vários existentes na norma considerada. A NBR ISO/IEC 17799 faz várias recomendações aos responsáveis que implementarão ou manterão a segurança da organização. As recomendações deverão ser selecionadas de acordo com sua necessidade e aplicabilidade [3].

A norma de segurança é dividida em 15 itens, cujos controles macros são:

- Política de Segurança.
- Segurança Organizacional.
- Classificação e Controle dos Ativos da Informação.
- Segurança Relacionada ao Pessoal.
- Segurança Física e do Ambiente.
- Gerenciamento de Operações e Comunicações.
- Controle de Acesso.
- Desenvolvimento da Segurança de Sistemas.
- Gestão da Continuidade do Negócio.
- Conformidade.

Cada um destes controles possui várias outras subdivisões conforme a

NBR ISO/IEC 17799, algumas premissas devem estar em conformidade com a Confidencialidade, Integridade e a Disponibilidade [14].

Os controles utilizados neste trabalho são: Política de Segurança, Segurança Organizacional, Segurança Relacionada ao Pessoal, Segurança Física e do Ambiente, Gerenciamento de Operações e Comunicações, Controle de Acesso e Gestão da Continuidade do Negócio [3].

Dentro do controle da Política de Segurança tem-se a necessidade de implementação de um processo de documentação que contenha tudo o que for definido na gestão da segurança da informação. A importância do comprometimento de todos funcionários neste processo e o material gerado deverão ser publicados por meio adequado a todos os colaboradores da empresa, URCTML.

É essencial que conste na documentação os objetivos gerais e a importância da gestão da segurança informação, o apoio claro e explícito da gerência e diretoria, uma breve e objetiva explicação sobre as políticas, padrões e normas que deverão ser seguidas.

O processo de revisão e manutenção periódica do sistema deverá ter um responsável que agirá de forma preventiva ou curativa a quaisquer sinais de riscos ou incidentes de segurança, como detecção de vírus e outros softwares que possam causar algum dano ao ambiente computacional como um todo [3].

A segurança organizacional objetiva um melhor gerenciamento da segurança da informação em uma organização. Todos os papéis deverão estar bem definidos e a contratação de uma consultoria de empresas terceirizadas são aspectos positivos na gestão da segurança. Toda revisão ou manutenção do sistema deve ser executada de forma imparcial para garantir que as políticas definidas estejam adequadas às práticas da organização. Caso seja necessário, deve-se contratar auditoria externa especializada.

O acesso de terceiros dentro das dependências da organização deve ser controlado e os riscos de acesso aos ativos da empresa analisados. Deve-se identificar o tipo e o motivo do acesso, seja ele físico (salas, computadores) ou

lógico (banco de dados, sistema de gestão da empresa) [3].

Empresas de suporte aos equipamentos e programas não necessitam de um acesso privilegiado como parceiros comerciais de auditoria contábil, que precisam acessar e em alguns casos, manipular informações da empresa com base nestas informações, aplicar políticas necessárias que estejam de comum acordo com as mesmas.

Com relação à segurança do pessoal, é importante treiná-los e educá-los, para que os mesmos se conscientizem, operando de forma adequada o meio computacional e minimizando os riscos de segurança. Diante desta conduta, é possível minimizar sensivelmente os incidentes [3].

A segurança física, envolve aspectos importantes dentro da organização, impedindo o acesso não autorizado. Uma organização das informações como: papéis e mídias eletrônicas no próprio local de trabalho pode diminuir consideravelmente acessos não autorizados ao sistema. Um perímetro de segurança é algo que constitui um obstáculo. Mais detalhes sobre as diretrizes de controle físico podem ser encontrados na Norma Internacional de gestão da segurança da informação, NBR ISO/IEC 17799 [3].

O controle de gerenciamento de comunicação e operações visa garantir uma segura e correta operação dos procedimentos da gestão de segurança. Procedimentos padrões para o gerenciamento de incidentes devem ter responsabilidades bem definidas. Quanto à cobertura dos riscos em potencial, alguns tipos podem ser:

- Falhas nos sistemas de gestão da informação e perda do serviço.
- Negação de serviço.
- Erros resultantes de dados com a integridade comprometida.
- Violação de confidencialidade.

Os tipos de planos de recuperação do sistema em casos de incidentes, podem ser:

- Diagnosticar e identificar das possíveis causas do incidente.
- Projetar ações que impeçam a duplicidade na ocorrência do incidente.
- Catalogar e documentar todas a ações e amostras dos incidentes.
- Informar a todos que foram afetados pelo incidente ou envolvidos com a recuperação dos dados.

Todas as provas devem ser recolhidas e guardadas com segurança para futuras análises do problema. Todas as ações de recuperação e correção de falhas, devem ser executadas de maneira formal e com critérios, tendo tudo documentado em detalhes, e com acesso apenas às pessoas devidamente autorizadas aos dados do sistema [3].

A proteção e controle contra *softwares* maliciosos também chamados de *malwares*[1], objetiva proteger a integridade das informações do sistema e alguns controles devem ser considerados:

- Proibir a instalação e utilização de *softwares* não autorizados.
- Transferência de arquivos ou *softwares* do meio externo para o ambiente corporativo e conscientizar sobre as formas e ações a serem tomadas nestes casos.
- Instalação e atualização periódica de *softwares* de anti-vírus e realizar treinamento para que os próprios colaboradores possam varrer quaisquer mídias eletrônicas que adentrem às dependências da empresa, prevenindo possíveis incidentes.
- Projetar tarefas que garantam a continuidade do negócio e a rápida recuperação no caso de incidentes.

O controle e gerenciamento da rede tem como objetivo a proteção da infra-estrutura, o perímetro e suas fronteiras, inserindo uma proteção extra às

1 Pequenos programas criados com o objetivo de executar tarefas maléficas em um ambiente computacional [13].

informações que trafegam pela rede através de controles de conteúdo [3].

O controle de acesso e suas políticas devem ser documentados e esclarecidos de forma explícita, os direitos de cada usuário através de declaração ou termo de compromisso com todos os requisitos a serem cumpridos. As regras podem ser aplicadas a um usuário ou a um grupo de usuários que possuem restrições em comum.

O gerenciamento do usuário, de seus privilégios e senhas também devem ter procedimentos formais e explícitos através do termo, atendendo todo o ciclo de vida do usuário que terá acesso ao sistema. Seu cadastramento deve possuir identificação única para uma melhor aplicação de privilégios e controles a cada função ou tarefa exercida pelo mesmo [3].

Após o cadastramento dos usuários, senhas e a aplicação dos privilégios necessários, deve-se monitorar o uso dos recursos do sistema, garantindo uma eficácia dos controles adotados e verificando se este está em conformidade com o modelo de política de acesso que fora definido. O monitoramento visa auditar horários de acesso ao sistema, identificar o usuário, identificar acessos que foram concedidos ou negados, programas e utilitário usados [3].

O gerenciamento da continuidade do negócio deve possuir mecanismos que possibilitam a identificação dos riscos, reduzindo-os e garantindo a retomada das atividades em tempo aceitável. Em posse destas informações, é possível verificar a conformidade com os requisitos [3].

5.3 Apresentação e Análise dos Resultados

Dentro do contexto da normativa NBR ISO/IEC 17799, há inúmeros controles que podem ser aplicados dentro de uma empresa, mas existem várias particularidades entre uma e outra, e nem sempre um controle deverá ser aplicado. Resumindo, não existe uma receita pronta para o Administrador de Redes utilizar e aplicar.

Para ser computada a pontuação e consequentemente conhecer o nível de recursos que deverão ser revistos, adaptados e ou implantados, quando um

item questionado atingir 100%, este valerá um ponto, 50% ½ ponto, 25% ¼ de ponto e 0% 0 ponto [6].

As tabelas utilizadas para reunir os resultados de cada item das políticas de segurança tiveram apenas como referência o *layout*, todas as perguntas, forma de pontuação e recomendações foram produzidas com base no ambiente computacional da empresa utilizada no estudo de caso e dados da empresa URCTML [6].

A tabela 2 apresenta três itens que foram questionados com relação às documentações que muitas vezes são esquecidas ou não é dada a devida importância por inúmeros administradores de rede.

A prática de documentação das políticas de segurança dentro da empresa tem como objetivo registrar tudo que for definido, para posteriormente servir como critério de cobrança. Registrar todas as políticas de segurança que deverão ser aplicadas, definir os papéis de cada funcionário, a forma mais clara possível nas quais deverão ser publicadas as documentações, a forma e a freqüência deverão ser avaliadas e atualizadas, são etapas indispensáveis. O apoio e o envolvimento da administração da empresa nesta etapa é de suma importância [6], [3].

Na tabela 2 sobre a documentação da política de segurança pode-se notar sensivelmente que há muito a ser feito.

Há a necessidade de se criar ou melhorar as documentações. A pontuação não foi satisfatória, pois a que poderia ser alcançada é de 7 pontos de acordo com o critério comentado anteriormente, mas somente pontuou 1 ponto [6], [3].

Documentação da Política de Segurança (Aderência Global)

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1. ADMINISTRAÇÃO E APOIO DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO							
1.1	A administração possui apoio e orientação em relação a segurança da informação?		x			25%	A administração deverá estar mais envolvida com a gestão da segurança

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1.2	A administração demostra seu compromisso e apoio, dentre as definições de controle da segurança da Informação?			x		50%	da informação da empresa.
2. DOCUMENTAÇÃO QUE DEFINIRÁ TODA AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO							
2.1	As Políticas aprovadas pela administração foram divulgadas a todos os colaboradores de maneira clara e de fácil acesso?	x				0%	É de suma importância que todas as Políticas de Segurança aprovadas pela administração, sejam publicadas de maneira acessível e com linguagem clara a todos os colaboradores da empresa. Também constando todos os direitos e deveres de cada colaborador.
2.2	Estão inclusos na documentação os objetivos e o escopo das Políticas de Segurança, uma breve explicação das políticas de segurança, e as consequências do não cumprimento às exigências que foram normatizadas?	x				0%	
2.3	Na documentação constam todas as responsabilidades pelo gerenciamento da segurança e notificação à pessoa responsável em caso de incidentes?	x				0%	
3. DOCUMENTAÇÃO DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO (REVISÃO E AVALIAÇÃO)							
3.1	Cada Política definida possui uma pessoa responsável em prestar manutenção e revisar de acordo com o que fora definido?	x				0%	Um gestor deverá ser definido, este será o responsável pela manutenção e revisão das Políticas de Segurança que foram definidas e aprovadas pela Direção.
3.2	Há revisões periódicas agendadas e validadas em relação a sua eficácia?		x			25%	Mesmo sem um gestor definido, existem procedimentos preventivos para minimizar as vulnerabilidades, porém serão mais eficazes criando-se um cronograma de todos os procedimentos.

Tabela 2: Controle da Norma NBR ISO/IEC 17799 - Documentação da Política de Segurança [6]

A tabela 3 apresenta dados em relação a administração organizacional da segurança dentro da empresa. Esta etapa está diretamente interligada com a etapa de documentação onde são validados os papéis e atribuições de cada pessoa envolvida e os cronogramas para a revisão das políticas definidas [6], [3].

Segurança Organizacional (Aderência Global)

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1. ADMINISTRAÇÃO ORGANIZACIONAL DA SEGURANÇA							
1.1	A administração organizacional está definida com os papéis e atribuições de cada pessoa envolvida?		x			25%	A administração deve ser mais envolvida e auxiliar nas definições dos papéis de cada um. Se necessário, deve-se contratar os serviços de consultoria de uma empresa externa. Um maior controle das revisões e manutenção deve ser implementado.
1.2	Há alguma empresa de consultoria que presta serviço terceirizado em relação a gestão da segurança, mantendo a empresa ou o gestor atualizado com as novidades?	x				0%	
1.3	As revisões e manutenções são ministradas de forma neutra e imparcial para garantir que as Politicas definidas estejam adequadas com relação às práticas?	x				0%	
1.4	O acesso físico e lógico de terceiros dentro das dependências da empresa está sendo monitorado e validado de acordo com as Políticas definidas?		x			25%	

Tabela 3: Controle da Norma NBR ISO/IEC 17799 - Segurança Organizacional [6]

No quesito Segurança Organizacional, também há uma alta deficiência, pois de 4 pontos possíveis de serem alcançados, apenas conquistou-se ½ ponto. A administração precisa estar mais presente nas definições dos papéis, solicitar consultoria externa se necessário, monitorar e validar o que for definido [6], [3].

Na tabela 4 são apresentados análise e resultados de questões de segurança envolvendo pessoas, por isso o envolvimento de todos os funcionários é muito importante. Treinamentos regulares devem ser realizados para auxiliar na conscientização e comprometimento de todos. Também é necessário um termo de compromisso com a confidencialidade das informações da empresa [6], [3].

Segurança Relacionada às Pessoas (Aderência Global)

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1. ADMINISTRAÇÃO DA SEGURANÇA ÀS PESSOAS							
1.1	São realizados treinamentos para a conscientização de todos sobre como proceder em caso de incidentes ou até mesmo em casos de suspeita de alguma ameaça dentro do meio computacional da empresa?			x		50%	Deve-se criar um cronograma das oficinas de reciclagens, mantendo assim, os colaboradores bem informados.
1.2	Existem revisões e atualizações periódicas destes treinamentos a fim de manter os colaboradores atualizados das novas ameças e de novas técnicas e procedimentos a serem tomados?		x			25%	
2. COMPROMISSOS DE CONFIDENCIALIDADE DAS INFORMAÇÕES							
2.1	São orientados todos os colaboradores sobre o compromisso de não divulgação de quaisquer informações confidenciais ou secretas que lhe são fornecidas?			x		50%	Convém que os termos de compromissos sejam atualizados, tornando-os assim mais abrangentes e cobrindo todo o meio computacional. Ou segmentá-los de forma que haja um termo para cada recurso existente.
2.2	O colaborador assina um termo de compromisso quanto à confidencialidade no momento em que lhe é fornecido acesso a algum recurso computacional da empresa?		x			25%	

Tabela 4: Controle da Norma NBR ISO/IEC 17799 - Segurança Relacionada às Pessoas [6]

Esta talvez seja uma das mais importantes etapas da implantação de Políticas de Segurança. De nada adianta toda a tecnologia de ponta, seja ela *hardware* ou *software* para proteger os perímetros de uma empresa, se não houver, conscientização, treinamentos, educação, apoio e compromisso com a causa dos colaboradores da empresa.

Dos 4 pontos possíveis, apenas 1 ½ ponto foi registrado. Uma atenção maior é necessária para estabelecer este controle à todos [6],[1].

Na tabela 5 são apresentados questões e resultados relativos à

segurança física do ambiente computacional, pois de nada adianta possuir vários mecanismos de controle de acesso e permissões ao sistema, se o local dos ativos críticos da empresa não estão em uma área restrita ou controlada [6], [3].

Segurança Física e do Ambiente (Aderência Global)

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** | **3:** Presença Total **(100%)d**
1. ADMINISTRAÇÃO DAS ÁREAS SEGURAS							
1.1	As áreas críticas da empresa estão em locais seguros e o perímetro está protegido com alguma barreira ou controle de entrada impedindo os acessos não autorizados?		x			25%	Perímetro deve ser definido e controles de acessos devem ser aprimorados evitando o acesso não autorizado.
1.2	Existe práticas de conservação de mesas e telas vazias para reduzir riscos de acesso não autorizado às informações da empresa ?			x		50%	Reforçar as necessidades dessas práticas nas oficinas de reciclagens.

Tabela 5: Controle da Norma NBR ISO/IEC 17799 - Segurança Física [6]

Não se conquista um boa segurança em um perímetro corporativo ou SOHO, se o acesso físico às informações não for composto de obstáculos que dificultem ou até mesmo impeçam o acesso. Controles mais rigorosos devem ser implementados. Dentre a pontuação a ser alcançada de 2 pontos, apenas 0,75 ponto foi computado [6], [3].

Gerenciamento das Operações e Comunicações (Aderência Global)

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1. PROCEDIMENTOS PADRÕES PARA GERENCIAMENTOS DE INCIDENTES							
1.1	Quanto a cobertura dos riscos em potencial como: Falhas no sistema, Negação de serviço, Integridade comprometida e violação de confidencialidade. Há procedimentos padrões de como agir definido?		x			25%	Procedimentos padrões preventivos ou curativos devem ser definidos. Se necessário, contratar uma consultoria externa antes.

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1.2	Quanto aos planos de recuperação do sistema, existe algum procedimento padrão definido?		x			25%	
2. ARMAZENAMENTO DAS PROVAS DE POSSÍVEIS INCIDENTES							
2.1	As provas de possíveis incidentes são armazenadas de forma segura para uma futura análise do problema que auxiliará na recuperação do sistema?	x				0%	Deve-se definir um local adequado para o armazenamento da documentação coletada de um possível incidente, se possível tudo em forma digital.
3. PROTEÇÃO E CONTROLE DE SOFTWARE MALICIOSO							
3.1	Há controles que impeçam a instalação e ou utilização de softwares não autorizados?			x		50%	É necessário melhorar o controle e as permissões dos usuários.
3.2	Há controles nas transferências de arquivos ou softwares do meio externo para o ambiente de produção da empresa?			x		50%	
3.3	São efetuados procedimentos de atualizações periódicas de softwares de anti-vírus e são fornecidas orientações aos colaboradores da importância de se varrer quaisquer mídias que adentrarem ao ambiente da empresa?				x	100%	Apesar desta tarefa já ser efetuada com certa regularidade, aconselha-se que o gestor de segurança e sua equipe, façam análises e certificações de que as tarefas estão sendo efetuadas.
3.4	Existem controles de conteúdo protegendo as informações que trafegam na rede?				x	100%	

Tabela 6: Controle da Norma NBR ISO/IEC 17799 - Gerenciamento das Operações e Comunicações [6]

A tabela 6 apresenta a análise e os resultados da comunicação, além do tráfego dentro da empresa. Há a necessidade da existência de planos de ação, possibilitando uma recuperação rápida das atividades fins da empresa caso haja algum incidente [6], [3].

A padronização de procedimentos é de suma importância para saber como agir em caso de incidentes. Políticas de armazenamento devem estar documentadas, bem como sua periodicidade, seu plano de recuperação ou contingência caso se tenha algum dado corrompido. Quanto à proteção lógica,

manter sempre o sistema atualizado e possuir mecanismos que aumentem a segurança do perímetro.

Percebe-se que este controle já possui uma efetividade regular, porém alguns pontos podem ser melhorados. Entretanto atingiu-se uma pontuação de 3,5 pontos dentre os 7 pontos possíveis de serem alcançados [6], [3].

Na tabela 7 são apresentados análise e resultados sobre o controle de acesso, esta etapa também está ligada à documentação. Através de um termo de compromisso, todos os funcionários devem estar totalmente esclarecidos em relação ao que terão ou não acesso, sobre o procedimento de como as senhas de acesso devem ser armazenadas e possuem características intransferível a outra pessoa. Auditorias periódicas devem ser realizadas com a finalidade de checar o uso correto do acesso concedido a cada funcionário, e para avaliar possíveis falhas ou vulnerabilidades no sistema [6],[3].

Controle de Acesso (Aderência Global)

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1. DOCUMENTAÇÃO E ESCLARECIMENTO QUANTO AO ACESSO							
1.1	As políticas de controle de acesso e os deveres de cada usuário são documentadas e esplanadas de forma clara através de termos de compromisso e ou declarações?			x		50%	A documentação deve ser melhorada e ter maior eficácia quanto aos esclarecimentos de controle de acesso.
1.2	O gerenciamento dos usuários, suas permissões e senhas são realizadas através de procedimentos padrões e esclarecidos através do termo ou da declaração?			x		50%	
2. FORMA DE IDENTIFICAÇÃO SEGUNDO AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO							
2.1	O cadastro dos usuários possui identificação única, permitindo um melhor controle das permissões para cada aplicação ou tarefa realizada?		x			25%	É papel do gestor de segurança garantir que seja realizadas uma política padrão de cadastramento, aplicação de

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
2.2	Após o cadastro dos usuários são feitas vistorias para checar se os privilégios e recursos definidos para cada usuário estão de acordo com as necessidades e em conformidade com o modelo de política adotado?	x				0%	permissões e auditorias do sistema periodicamente a fim de mensurar os possíveis riscos em que a empresa esteja exposta.
2.3	São realizados auditorias periódicas para checar horários de acesso, pedido de acessos negados ou permitidos e programas utilizados por cada usuário?	x				0%	

Tabela 7: Controle da Norma NBR ISO/IEC 17799 - Controle de Acesso [6]

Neste controle da Norma NBR ISO/IEC 17799, que também é referenciada no nível de segurança C2, trata-se das políticas do controle de acesso ao sistema por parte dos usuários.

Após definidas as contas de cada usuário, é fundamental que haja um termo ou declaração completa, onde sejam especificados de maneira clara, todos os direitos e deveres a serem seguidos. A identificação dos usuários deve ser coesa.

Após esta etapa, uma rotina de verificação dos acessos, quanto a horários, sessões permitidas e ou negadas dos aplicativos devem ser validadas para certificar que as permissões definidas estão adequadas. No total de 5 pontos, foi conseguido 1 ¼ pontos, portanto, deve ser melhorado [6].

A tabela 8 apresenta análise e resultados das questões sobre a continuidade do negócio, ou seja, manter as atividades fins da empresa funcionando [6], [3].

Conformidade e Continuidade do Negócio (Aderência Global)

Item	Questões a serem avaliadas	Peso				Pontos	Legenda ou Observações
		0	1	2	3		**0:** Ausência **(0%)** **1:** Presença Não Eficiente **(25%)** **2:** Presença Parcial **(50%)** **3:** Presença Total **(100%)**
1. MANTENDO A CONTINUIDADE DO NEGÓCIO							
1.1	Existem mecanismos que auxiliam na identificação dos riscos, para que esses possam ser reduzidos e também garantir uma recuperação ou retomada de todas ou parte parte principal das atividades em menor tempo possível?		x			25%	Mecanismos devem ser criados para agir de forma preventiva. Quanto à recuperação do sistema, as políticas de backup existentes nem sempre contemplam a necessidade da empresa de uma retomada das atividades de forma rápida.
2. CONFORMIDADE COM OS REQUISITOS							
2.1	Em poder das informações geradas pelo mecanismo citado anteriormente, é possível a verificação de conformidade com os requisitos e políticas adotadas?		x			25%	O gestor de segurança deve criar um cronograma de validação das políticas e conformidades adotadas.

Tabela 8: Controle da Norma NBR ISO/IEC 17799 - Conformidade e Continuidade do Negócio [6]

Após todos os controles é o momento para avaliar de que forma o negócio da empresa permanecerá em funcionamento. Para isso, deve-se possuir mecanismos capazes de mensurar os possíveis riscos e interceptá-los, aumentando, assim, sua disponibilidade.

Estes mecanismos e todas as políticas adotadas devem estar em conformidade com as normas e requisitos definidos. Caso haja alguma divergência, deve-se reavaliar, reestruturar e publicar novamente. A pontuação deste controle atingiu ½ ponto dos 2 pontos possíveis [6], [3].

5.4 Resultados Obtidos

Os critérios para a análise e apresentação da avaliação foram obtidos através de pontuações de 0 a 3, sendo 0 ausência (0%), 1 presença não eficiente (25%), 2 presença parcial (50%) e 3 presença total (100%) de aderência à alguma das normas ou itens das normas [6], [3].

Na análise sobre a documentação existente na empresa, notou-se a

necessidade de melhoraria do envolvimento da administração quanto à gestão da segurança deixando bem claro sua importância e definindo uma pessoa responsável para manter tais documentações. Neste quesito avaliou-se 7 itens e aproximadamente 14% já estão implementados [6], [3].

Na análise de segurança organizacional verificou-se que existem deficiências envolvendo a administração. Esta deve estar mais presente e é importante a definição dos papéis de cada envolvido. O processo de monitoração e validação que for definido poderá ser feito por terceiros. A pontuação ficou próximo de 12% já implementado [6], [3].

A análise da segurança pessoal obteve um bom resultado. Alguns treinamentos já foram realizados com o objetivo de conscientizar os funcionários da empresa. Uma sugestão, seria criar um projeto onde a mudança e reciclagem das informações a serem passadas estejam em permanente adequação. Esta análise conquistou aproximadamente 30% e foi efetivada ou implementada [6], [3].

Na segurança física do ambiente computacional deve-se aumentar o controle de acesso à áreas críticas da empresa e manter informações sigilosas em locais seguros e fora do alcance de pessoas não autorizadas. A pontuação deste quesito alcançou aproximadamente 40% de recursos já utilizados ou implantados [6], [3].

No gerenciamento das operações e comunicação houve uma surpresa, pois no momento da análise, algumas tarefas já eram executadas. As documentações de possíveis incidentes, procedimentos padrões de como agir e como armazená-los, devem ser revistos e melhorados. A pontuação foi de 50% de aderência [6], [3].

Em conformidade com a continuidade do negócio, recomenda-se criar mecanismos preventivos para atuar em possíveis desastres, redundância e integridade dos dados os quais fora realizado o backup, critérios de recuperação rápida e formas de testar regularmente através de um cronograma a eficiência dos mecanismos. A pontuação deste item alcançou 25% [6], [3].

6. Conclusão

6.1 Considerações Finais

Este capítulo encerra o trabalho apresentando os resultados obtidos após a análise e todas as propostas de mudanças. A proposta deste trabalho foi alcançada, pois fora mostrada a importância em manter as informações mais seguras, técnicas sobre como melhorar a segurança, controle de acesso e sugestão de mudança do layout do perímetro de rede e na topologia, minimizando riscos à integridade dos dados da empresa.

Por coincidência, a empresa do estudo de caso, possui uma agência que regulamenta praticamente todas as suas atividades fim, e no decorrer deste trabalho, esta agência criou uma normativa que determinava algumas normas e padrões que deveriam ser adotados pela empresa URCTML e outras co-irmãs para garantir a integridade das informações. Um dos vários padrões a serem adotados é a NBR ISO/IEC 17799, e isso contribuiu muito para o enriquecimento deste trabalho, tornando-o viável e possível a sua implementação de fato no ambiente estudado.

A comprovação de que algumas políticas mesmo que parcialmente já estavam implementadas na empresa URCTML no momento desta análise, demostra que a preocupação das empresas e dos profissionais que gerem a segurança da informação é realidade, mesmo que neste caso, não foram obedecidos alguns critérios, seguida alguma norma ou padrão para a sua implementação, demostrou alguma eficiência mesmo que pouca. Tomar conhecimento deste fato serviu como incentivo, pois significa que a empresa não está tão fora do caminho da conquista de seus objetivos com relação à segurança de seus dados e obedecendo às determinações impostas pela agência reguladora, porém ainda há muito a ser feito. Como proposta de trabalhos futuros, poderá ser criado um live-CD interativo que auxilie o administrador de redes a criar tal ambiente, de forma automatizada.

7. Referências Bibliográficas

7.1 Livros

[1] TRIGO, Clodonil Honorio. MELO, Sandro. *Projeto de Segurança em Software Livre: Linux Seguro – Firewall – Proxy – Identificadores de Intrusos (IDS) – Rede Privada (VPN).* São Paulo: Editora Alta Books, 2004. 193p.

[2] SOARES, Luiz Fernando Gomes. LEMOS, Guido. COLCHER, Sérgio. *Rede de Computadores: Das LANs, MANs e WANs às Redes ATM.* Rio de Janeiro: Editora Campus, 1995. 705p.

[3] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR-ISO/IEC 17799:2005: *Tecnologia da Informação – Técnicas de Segurança - Código de Prática para Gestão da Segurança de Informações. Rio de Janeiro,* 2005, 120p.

[4] MELO, Sandro. DOMINGOS, Cesar. CORREIA, Lucas. MARUYAMA, Tiago. *BS7799: Da Tática à Prática em Servidores Linux.* Rio de Janeiro: Editora Alta Books, 2006. 232p.

7.2 Monografias

[5] GONÇALVES, Luís Rodrigo de Oliveira. *Um Modelo para Verificação, Homologação e Certificação de Aderência à Norma Nacional de Segurança de Informação - NBR-ISO IEC-17799. 2005. 189 f.* Dissertação (Mestrando em Ciências em Engenharia de Sistemas e Computação) – Universidade de Engenharia de Sistemas e Computação, Universidade Federal do Rio de Janeiro, Rio de Janeiro.

[6] SALGADO, Ivan Jorge Chueri. BANDEIRA, Ronaldo. SILVA, Rivanildo Sanches. *Análise de Segurança Física em Conformidade com a Norma ABNT NBR ISO/IEC 17799.* 2004. 326 f. Monografia (Graduandos em Tecnologia em Segurança da Informação) – Faculdade em Tecnologia em Segurança da Informação, Faculdades Integradas ICESP, Brasília.

7.3 Webibliografias

[7] NETFILTER, Netfilter - firewalling, NAT, and packet mangling for Linux. [on-line]. Disponível na Internet via www. url: http://www.netfilter.org. Arquivo capturado em 20, de Julho de 2006.

[8] BERTELLA, Marcio Luís. TONIN, Neilor Avelino. *A Implementação de uma Rede de Computadores com os Sistemas Operacionais Unix e WindowsNT Utilizando o Protocolo TCP/IP e o Gerenciador de Arquivos Distribuídos NFS.* [on-line].Disponível na Internet via www. url: http://www.inf.uri.com.br/implementacao.htm. Arquivo capturado em 22, de Julho de 2006.

[9] ABSOLUTA. *Padrões para Segurança de Computadores (TCSEC, ITSEC E CC).* [on-line]. Disponível na Internet via www. url: http://www.absoluta.org/seguranca/seg_padroes.htm. Arquivo capturado em 20, de Julho de 2006.

[10] MODULO, Portal do Profissional da Segurança da Informação. [on-line]. Diponível na Internet via www. url: http://www.modulo.com.br. Arquivo capturado em 05, de Setembro de 2006.

[11] ATAÍDE BARBOSA MARTINS, Uma abordagem Metodológica Baseada em Normas e Padrões de Segurança. Estudo de Caso CETREL S/A. [on-line]. Disponível na Internet via www. url: http://www.linorg.cirp.usp.br/SSI/SSI2004/Poster/P03_ssi04.pdf. Arquivo capturado em 12, de Agosto de 2006.

[12] SANDRO MELO e TIAGO MARYAMA, Tutorial de Lids – Versão 0.1 (Lids – Linux Intrusion Detection System). [on-line]. Disponível na Internet via www. url: http://arl.ginux.ufla.br/moodle/mod/resource/view.php?id=439. Arquivo capturado em 27, de Julho de 2006.

[13] WIKIPÉDIA, A Enciclopédia Livre. [on-line]. Disponível na Internet via www. url: http://pt.wikipedia.org. Arquivo capturado em 15, de Agosto de 2006.

[14] ATAÍDE BARBOSA MARTINS e CELSO ALBERTO SAIBEL SANTOS, Uma Metodologia para a Implantação de um Sistema de Gestão de Segurança da

Informação. [on-line]. Disponível na Internet via www. url: http://www.tecsi.fea.usp.br/revistatecsi/edicoesanteriores/v02n02-2005/pdf/a02v02n02.pdf. Arquivo capturado em 05, de Setembro de 2006.

[15] THE PAX TEAM, Homepage of The PAX Team. [on-line]. Disponível na Internet via www. url: http://pax.grsecurity.net. Arquivo capturado em 20, de Fevereio de 2007.