

# Utilizando Linux Brazilfw como Roteador/firewall e Gerenciador da Rede em Unidades Escolares da Rede Estadual de Santa Catarina

Werner Bruns  
werner.bruns@gmail.com  
Unidavi

Fábio Alexandrini  
fabalexandrini@yahoo.com.br  
Unidavi-IFC-Rio Sul

Carla F D Alexandrini  
carla\_alex10@hotmail.com  
Unidavi

José Ernesto De Faveri  
faveri@unidavi.edu.br  
Unidavi

Thiago Souza Araujo  
prof.araujo@unidavi.edu.br  
Unidavi-USJ

**Resumo:** Este artigo trata-se da necessidade da implementação de um sistema de segurança, que permita bloquear o acesso aos conteúdos indesejados oriundos da internet e o gerenciamento da mesma, numa escola da rede pública estadual. Os recursos tecnológicos como a internet e a Tecnologia da Informação (Informática) são ferramentas importantes para o auxílio a didática aos alunos. Estes possuem um leque de informações e de possibilidades que quando bem orientadas são de uma consistência ampla para conhecimentos, que pode enriquecer ainda mais o processo de ensino e aprendizagem. O objetivo desse artigo é de manter conteúdos de alto nível para o conhecimento e orientar professores e alunos quanto à importância do uso correto e planejado dos recursos disponíveis para o aprendizado escolar. Assim viu-se a necessidade da implantação / Instalação de um sistema de segurança de rede chamado BrasilFW. Dentre algumas pesquisas, decidiu-se pela implantação do sistema para assegurar a pesquisa e navegação a conteúdos que atenda as necessidades da escola. O BrasilFW, possibilita melhorar o desempenho do link de internet, filtrar conteúdos acessados, agendar a utilização de serviços de mensagens e o acesso às redes sociais, obtendo assim um planejamento e orientação para os trabalhos escolares.

**Palavras Chave:** Rede Escolar - Tec.Inf.Comunicação - Segurança Informação - Educação Tecnológica - Escola Estadual



## **INTRODUÇÃO**

Este artigo foi realizado na Escola de Educação Básica Leopoldo Jacobsen, situada no bairro Seminário na cidade de Taió – SC, com o objetivo principal de instalar um roteador / servidor de internet com um sistema operacional de rede Linux, para gerenciar e monitorar o acesso à internet com uma distribuição livre e gratuita.

Com isso apresentaremos neste artigo uma solução para segurança de redes públicas desenvolvida para proteção de dados, focando-se nas necessidades para aprendizagem dos alunos e adequando-se à estrutura da escola existente. Essa solução é uma ferramenta que se chama BrasilFW.

Esse artigo tem como objetivo mostrar como é possível o monitoramento e a administração de conteúdos na rede mundial chamada Internet, mostrando alternativa de controle de dados e acessos realizados pelos professores e alunos, concentrando a passagem de dados em um único local, assim obtendo o controle na manutenção do link de internet e a manipulação da informação da entidade, disponibilizando os acessos de forma segura.

O tema em questão tem importância significativa não só, devido aos padrões de segurança da tecnologia da informação, mas também, mostrar a aplicação Firewall (BrasilFW) para o controle da educação e aprendizagem a Escola de Educação Básica Leopoldo Jacobsen.

A Escola de Educação Básica Leopoldo Jacobsen dispõe de computadores e acesso a internet, e que foi recebida através do programa ProInfo. A sala de informática é utilizada preferencialmente para pesquisa a conteúdos educativos, de forma a dar um suporte pedagógico diferenciado e tornar as aulas mais produtivas e interativas, assim ultrapassando os limites da biblioteca da escola. Outros fatores importantes também são o reduzido número de livros que pode ser insuficiente para atender a turma e, eventualmente, o conteúdo desatualizado como, por exemplo, as revisões de alguns exemplares constantes no acervo da escola.

O Programa Nacional de Tecnologia Educacional (ProInfo). É um programa educacional com o objetivo de promover o uso pedagógico da informática na rede pública de educação básica. O programa leva às escolas computadores, recursos digitais e conteúdos educacionais. Em contrapartida, estados, Distrito Federal e municípios devem garantir a estrutura adequada para receber os laboratórios e capacitar os educadores para uso das máquinas e tecnologias. (MEC 2011).

A EEB Leopoldo Jacobsen apresentada na figura 1 abaixo, é uma escola de Ensino Fundamental até Ensino Médio, além da unidade do CEJA ocupando o espaço cedido, com o total de 381 de alunos no Ensino Fundamental, de 201 no Ensino Médio, também está iniciando 3 turmas da 1ª fase do projeto de Ensino Médio Inovador e além dos 116 alunos do Ceja.



**Figura 1:** Hall

de entrada da EEBLJ

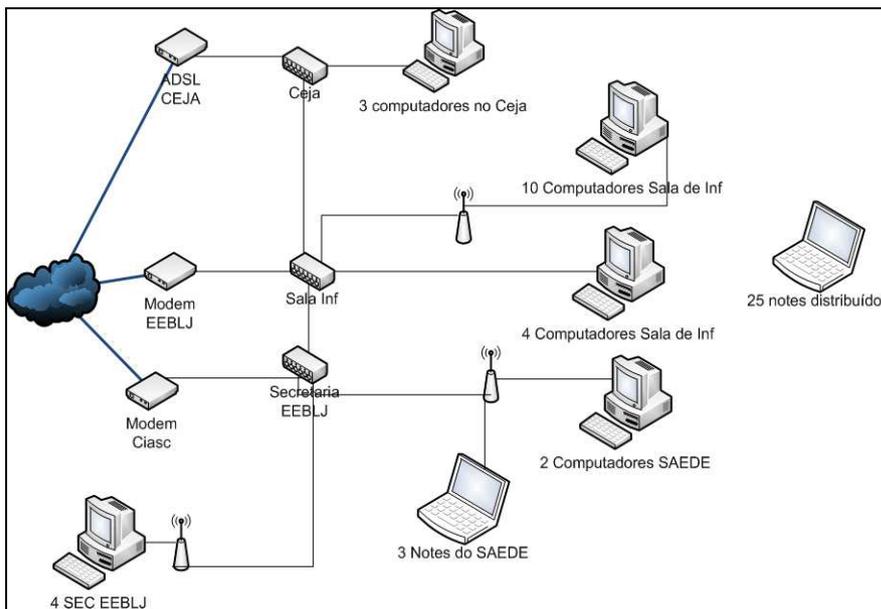
**Fonte:** Acervo do autor.

Conta com um laboratório de Informática, conhecido também como sala de Tecnologia Educacional com 10 computadores do Proinfo Urbano FNDE 2007 pregão 45, e 4 computadores da marca Braox com windows 7 e office 2007.

Tem se também a sala conhecida como SAEDE para as crianças especiais, onde tem dois computadores e três notebooks com programas específicos para alunos com alguma deficiência auditiva ou de visão, sendo que alguns destes programas usam a internet.

A Secretaria da EEBLJ, conta com quatro computadores da marca Braox com Windows 7 e Office 2007. A Secretaria do CEJA, conta com três CPUs com Windows 7 e Office 2007, e no geral tem em torno de dez notebooks dos professores e uns 15 notebooks/netbooks de alunos.

A Figura 2 demonstra a estrutura rede da EEBLJ antes da implementação do BrazilFW, onde nesta configuração, a rede é usada de forma compartilhada com dois links do MEC (2048 Kbps) e um link do CIASC (512 Kbps), configurado manualmente os ips em cada computador e notebook, usando-se três switch e três AP (ponto de acesso Wireless).



**Figura 2:** Escopo EEBLJ.

**Fonte:** Acervo do autor.

Conforme a figura 2 existe a dificuldade de controlar o acesso, o gerenciamento, vírus, lentidão, perda de conexão e o tráfego da rede. Sendo neste momento necessário encontrar uma solução para o problema acima.

No desenvolvimento será descrito os conceitos de alguns métodos utilizados e a implantação da ferramenta utilizada. Diversos conceitos tratados nesse artigo são descritos. Tais conceitos são essenciais para a compreensão dos modelos e padrões associados à Gestão de Riscos e à Firewall.

## **GESTÃO DE RISCOS**

“Ela ultrapassa a análise de vulnerabilidades, em atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos” (ISO, 2002). A mesma envolve um processo criterioso e recursivo de documentação, avaliação e decisão durante todas as faces do ciclo de vida do projeto.

### **Segurança em Redes**

Segurança em tecnologia da informação é definida como: “a capacidade de assegurar a prevenção ao acesso e à manipulação ilegítima da informação, ou ainda, de evitar a interferência indevida na sua operação normal” (ISO, 2005). A segurança é fundamentada em três propriedades básicas (BISHOP, 2003):

- **Integridade:** garante que a informação não será alterada ou destruída sem a autorização adequada.
- **Confidencialidade:** garante que a informação não será revelada sem a autorização adequada.
- **Disponibilidade:** garante que a informação estará acessível aos usuários legítimos quando solicitada.

### **Violações de Segurança**

Quando há quebra de uma ou mais propriedades de segurança, há uma violação de segurança. Portanto, como as violações estão relacionadas com três propriedades básicas, as mesmas podem ser classificadas também em três categorias:

- Revelação não autorizada da informação (violação de confidencialidade);
- Modificação não autorizada da informação (violação de integridade);
- Negação de serviço (violação de disponibilidade).



## Vulnerabilidade

“Uma vulnerabilidade é um defeito ou fraqueza no design ou na implementação de um sistema de informações, que pode ser intencionalmente ou acidentalmente explorada, afetando a confidencialidade, integridade ou disponibilidade” (ROSS, 2008).

## Ameaças, Ataques e Intrusão.

Uma ameaça é: “qualquer circunstância ou evento com o potencial intencional ou acidental de explorar uma vulnerabilidade específica em qualquer sistema computacional, resultando na perda de confidencialidade, integridade ou disponibilidade” (BARKER e LEE, 2004).

## Risco

“É o impacto negativo da exploração de uma vulnerabilidade, considerando a probabilidade do uso do mesmo e o impacto da violação” (STONEBURNER, et al, 2002). Ou seja, são as violações e prejuízos que podem acontecer.

## FIREWALL

Uma definição convencional: Parede corta fogo. Dispositivo feito de material a prova de fogo para evitar que o fogo se espalhe de uma parte do edifício para outra.

Uma definição para sistemas computacionais: “Ponto de controle que mantém acessos não autorizados fora do perímetro de segurança, ao mesmo tempo possibilita acesso aos sistemas externos” (PFLEEGER, 2006).

- Atua como uma barreira de segurança entre a rede interna e o mundo exterior.
- Evita que potenciais vulnerabilidades de serviços sejam exploradas, nisso pode-se dizer que não exista nenhum software 100% seguro.
- Pode ser classificado como firewall:
  - De máquina ou,
  - De rede.

## Firewall de Máquina

Sua segurança é a própria máquina, assim tem-se:

- Análise de todo o tráfego que entra e que sai.
- As regras podem seguir uma política de segurança da organização ou o próprio usuário pode definir suas regras, um exemplo, Firewall do Microsoft Windows.
- A Figura 3 mostra um computador doméstico, de uso pessoal que está conectado a internet.





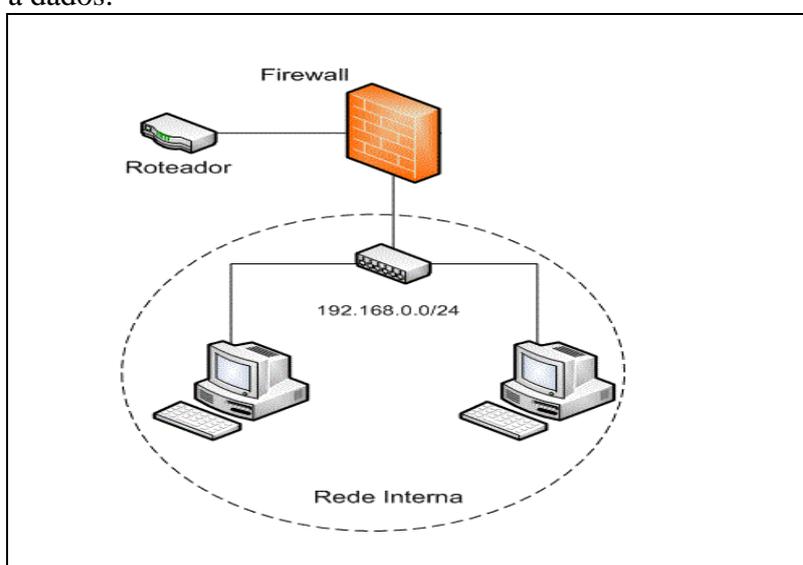
**Figura 3:** Firewall Microsoft Windows.

**Fonte:** Acervo do autor.

### Firewall de Rede

Segundo Pfleeger (2006), rede local de uma organização, engloba:

- Análise de todo o tráfego de dentro para fora e de fora para dentro, deverá passar pelo Firewall;
- Somente o tráfego autorizado, definido pela política de segurança local, deverá ter permissão para passar;
- O próprio Firewall deverá ser imune a invasões, implicando na utilização de um sistema confiável, com um sistema operacional seguro e rodando um conjunto mínimo de serviços.
- A Figura 4 ilustra uma rede com acesso a internet, ataques / invasões e acesso a dados.



**Figura 4:** Firewall.

**Autor:** Acervo do autor.

### Tipos de Firewall

Segundo Rodrigues (2012), temos os seguintes tipos:

- Os **filtros de pacotes** atuam na camada de rede e não se preocupam com o conteúdo dos pacotes. Analisa todos os dados que passa e decide se será descartado ou encaminhado. Preocupa-se com os endereços e portas de origem e destino e protocolo utilizado, geralmente combinado com um roteador.
- **Inspeção de estado** atua na camada de transporte, não analisa pacotes individuais, mantém estado de todas as conexões que passam e consegue determinar se um pacote faz parte de uma conexão existente ou de uma nova conexão.
- **Gateway** atua na camada de aplicação, examinando o conteúdo dos pacotes e permitindo um controle mais granular, exemplo, aos usuários internos não é permitido baixar arquivos (.EXE). Este consome uma carga maior de processamento e a conexão entre clientes e servidores é sempre intermediada.

## ROTEADORES



Segundo (RODRIGUEZ, et al, 2000), “roteadores são equipamentos utilizados para conectar duas ou mais redes, permitindo o redirecionamento do tráfego de rede através de um endereço lógico”.

Segundo (ROSS, 2008), “são equipamentos que trabalham com a camada 1,2 e 3 do Modelo ISO/OSI”. Através de regras inseridas conhecidas como rotas estáticas, regras dinâmicas aprendidas através de protocolos de roteamento usados entre roteadores como o RIP, OSPF, etc.

Ainda segundo (ROSS, 2008), “na prática, os roteadores são utilizados para redirecionar pacotes entre redes remotas”. Os roteadores são capazes de interpretar informações complexas de endereçamento e tomar decisões sobre como encaminhar os pacotes através dos links que interligam as redes, além de poder incluir ou alterar as informações dos pacotes para que cheguem ao destino.

## **BRASILFW**

Segundo (BRAZILFW, 2011) “é uma mini distribuição Linux que destina ser um Firewall e Roteador, baseado no Coyote Linux que foi descontinuado. Originalmente cabia num disquete, mas com a necessidade de um serviço de servidor proxy passou sua execução para um disco rígido”.

Atualmente existem duas versões:

- 2.x.x que tem como base o Kernel 2.4.x do Linux.
- 3.x.x que tem como base o Kernel 3.x.x do Linux.

Apesar da versão 2.x.x terem diversos complementos que o deixa mais completo, a versão 3.x.x está em sendo desenvolvido a partir do zero, e os complementos aos poucos vão sendo adaptados e migrados para a nova versão.

## **Desenvolvimento do Trabalho**

Ferramenta Implementada foi sugerida pelo NTE<sup>1</sup> de Taió-SC, devido as características do equipamento<sup>2</sup> disponível na escola para a sua utilização como provedor da solução. A ferramenta foi instalado neste equipamento em agosto de 2011 com configurações mínimas para o seu funcionamento como roteador. Sua instalação levou em torno de 8 horas desde a instalação até o seu funcionamento inicial. Durante o segundo semestre de 2011, foi estudado e configurado o seu firewall, proxy e roteamento avançado conforme a necessidade de soluções cotidianas, como por exemplo: bloqueio de jogos on-line, monitoramento de acesso a páginas web em tempo real de equipamentos específicos.

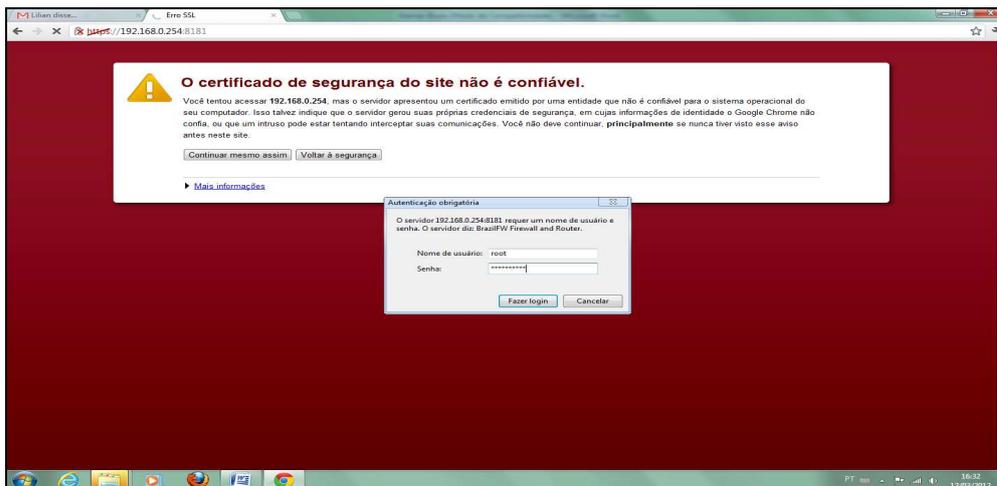
A ferramenta serve de base para o desenvolvimento e andamento de uma solução para proteção de dados, focando-se nas necessidades para aprendizagem dos alunos e adequando-se à estrutura da escola existente. Essa solução é uma ferramenta que se chama BrasilFW.

Na figura 5 mostra a entrada de login, onde existe uma chave SSL autônoma que garante a autenticação segura e confiante.

---

<sup>1</sup> NTE – Núcleo de Tecnologia Educacional, é uma estrutura desconcentrada, vinculada a Gerencia da Educação, da Secretaria de Estado de Desenvolvimento Regional – SDR, subordinada à Gerencia de Educação, da Secretaria de Estado da Educação de Santa Catarina, e especializado em tecnologia da informação e comunicação (TIC) aplicado à educação.

<sup>2</sup> Computador PC Pentium 4 com 512 MB de memória e 80 G de Hard Drive.

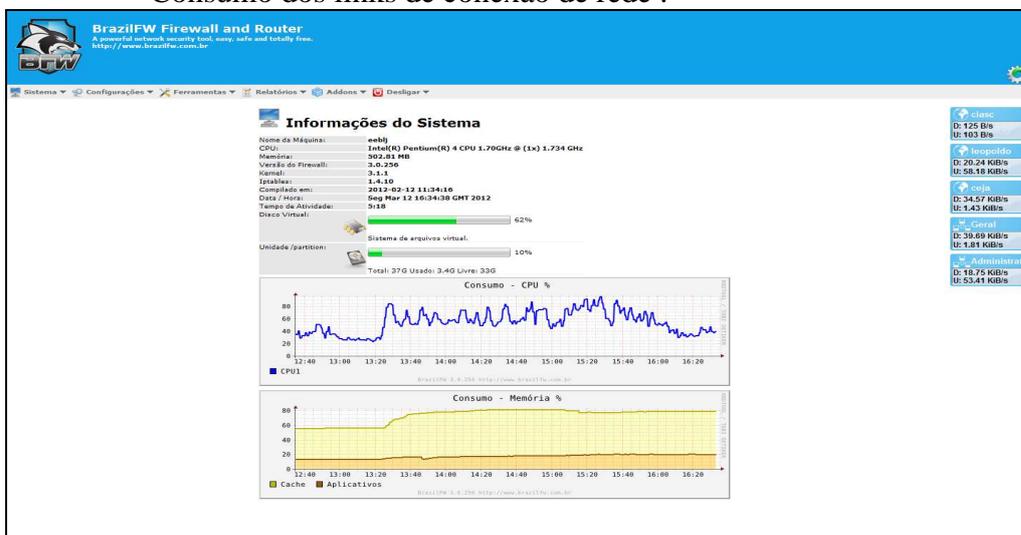


**Figura 5:** Entrada de login.

**Autor:** Acervo do autor.

Realizando essa autenticação, iremos à tela inicial do sistema, demonstrando algumas informações, como mostra a figura 6, temos informações básicas como:

- Nome do servidor;
- Versão;
- Uso da unidade de armazenamento;
- Histórico de consumo da CPU e da Memória;
- Consumo dos links de conexão de rede .



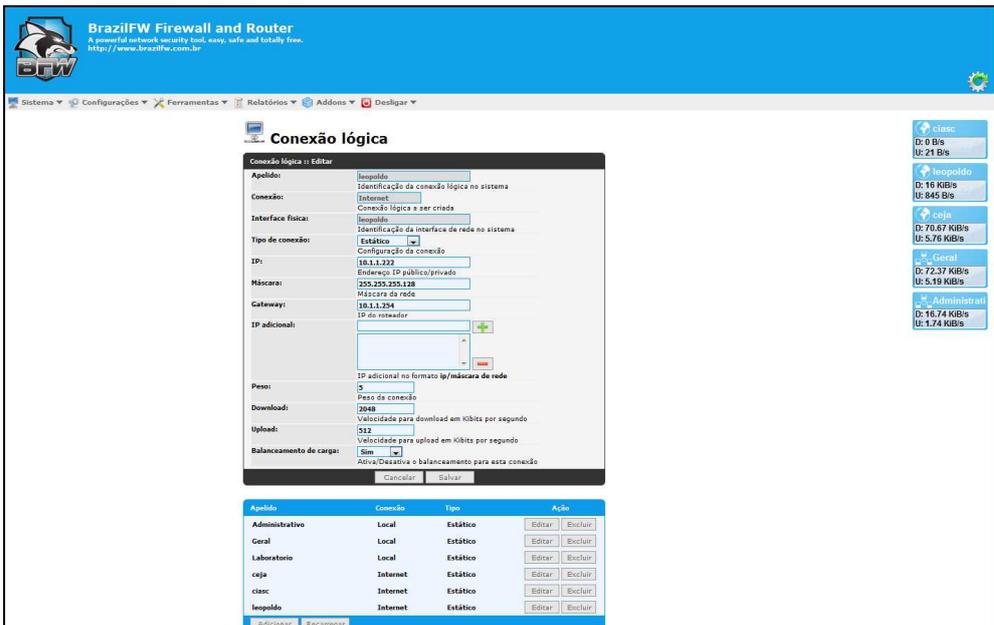
**Figura 6:** Informações do Sistema.

**Autor:** Acervo do autor.

Na figura 7, demonstrou-se a conexão lógica via internet, neste ponto define-se a conexão com a internet, onde se tem várias opções como pppoe, cliente dhcp, estático, etc. Esta conexão está definida como estática, com as informações da velocidade da conexão, com capacidade de balanceamento de carga e seu peso, já que a mesma possui outras duas conexões com a internet para balanceamento de carga com velocidades diferentes.

Na verdade as configurações são parâmetros dos comandos do pacote iproute2<sup>3</sup> que implanta a configuração e roteamento de rede no kernel do linux.

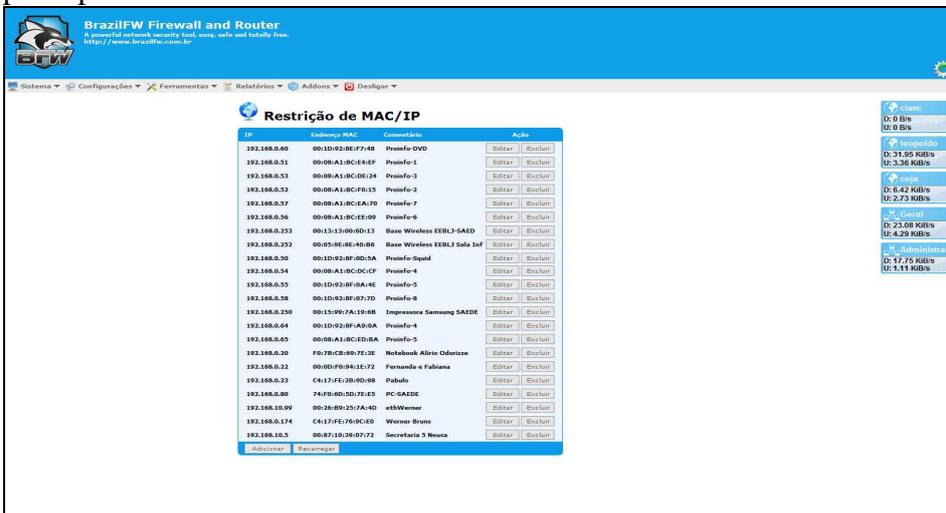
<sup>3</sup>iproute2 é uma coleção de utilitários de controle de rede e tráfego de TCP/IP no linux.



**Figura 7:** Conexão lógica.

**Autor:** Acervo do autor.

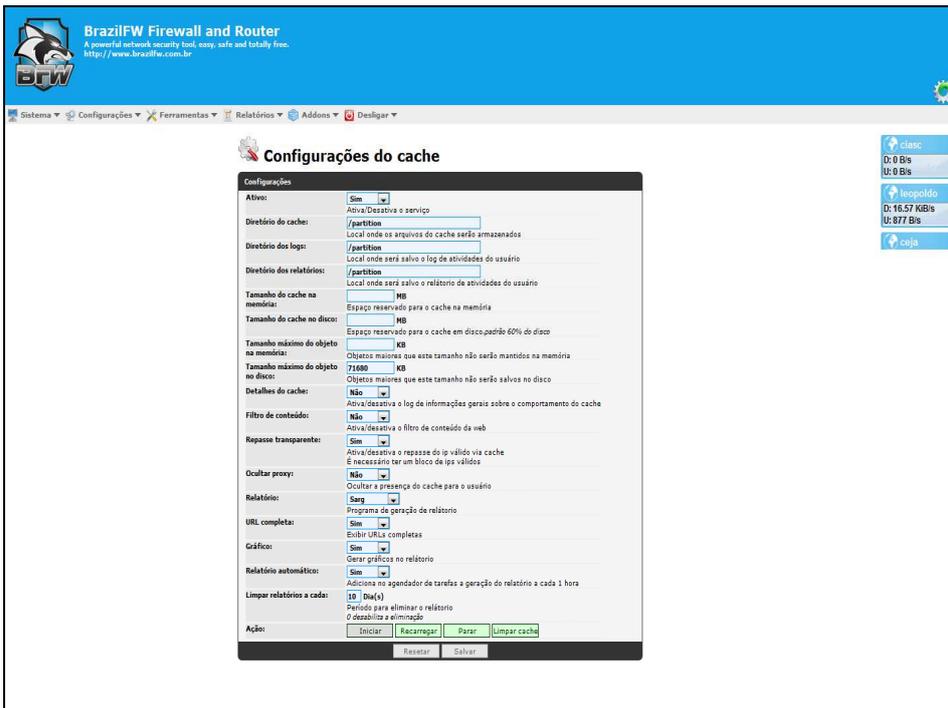
Realizando a conexão lógica, na figura 8 configura-se e atribuiu-se IPs estáticos a determinados computadores e Periféricos através do MAC address, sendo os mesmos utilizados futuramente para autorização e o monitoramento de acesso e consumo da rede, principalmente o acesso à internet.



**Figura 8:** Restrição de MAC/IP.

**Autor:** Acervo do autor.

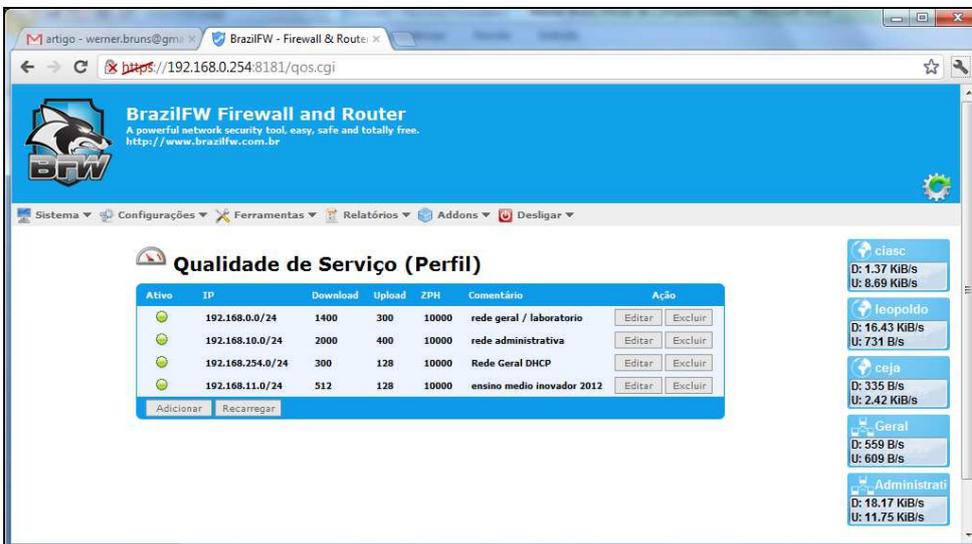
Com as restrições configuradas seguiu-se para as configurações básicas do servidor de proxy squid demonstrada na figura 9, sendo estas servem para indicar o tamanho, o local de armazenamento dos dados do cache, dos logs, se utiliza ou não sistema de relatórios como o SARG.



**Figura 9:** Configurações do cache no Serviço Proxy Squid.

**Autor:** Acervo do autor.

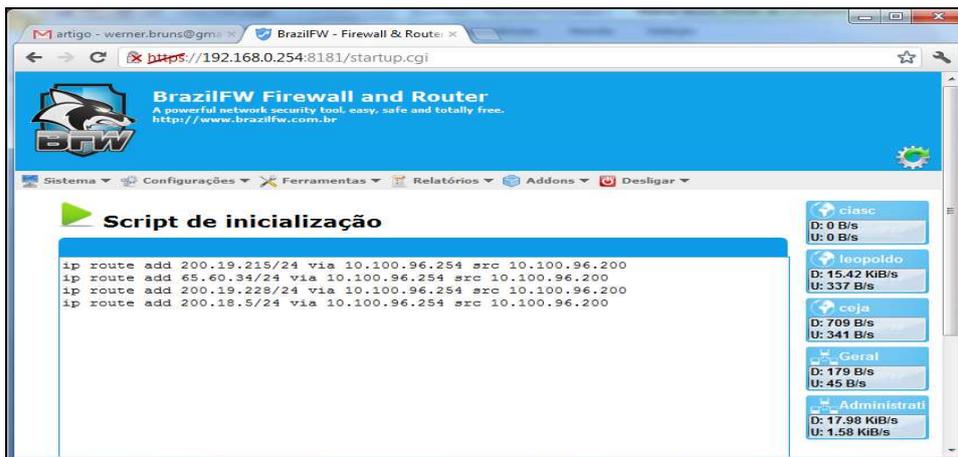
Configura-se um balanceamento de carga da rede interna (figura 10), desta forma consegue-se distribuir a internet para todos, sem denegrir o desempenho no laboratório e da rede administrativa.



**Figura 10:** Qualidade de Serviço (QOS).

**Autor:** Acervo do autor.

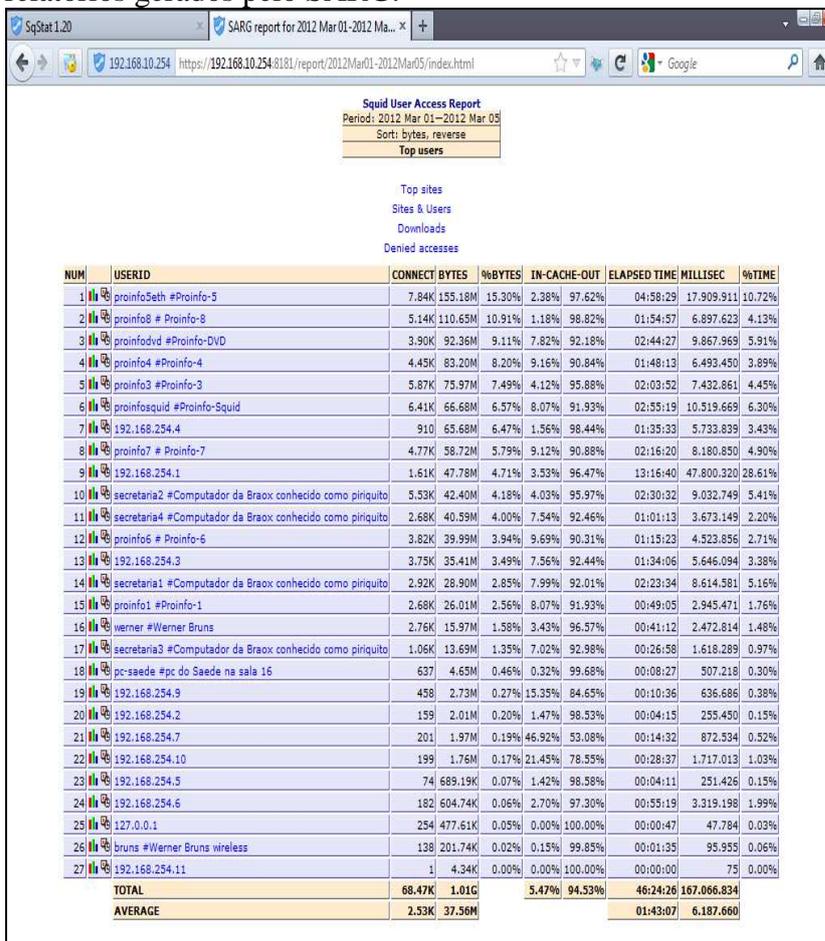
O script de inicialização é um arquivo de inicialização de comandos personalizados como demonstrado na figura 11, neste caso, é incluído um roteamento estático para a rede do governo de Santa Catarina, desta forma, somente passa pela rede do estado o que é necessário.



**Figura 11:** Script de inicialização.

**Autor:** Acervo do autor.

Na figura 12 pode-se ver as estatísticas e histórico de uso dos dias anteriores via os relatórios gerados pelo SARG.



**Figura 12:** SARG.

**Autor:** Acervo do autor.

Na figura 13, se pode ver a utilização das conexões http via servidor proxy e o consumo de trafico por máquina no instante do acesso via a ferramenta conhecida como SqStat 1.20.

Esta ferramenta permite visualizar quais sites estão sendo acessados, podendo identificar a origem do acesso e seu consumo. Desta forma, o administrador pode identificar

se os conteúdos estão condizentes, ou se esta havendo acessos indevidos, não reconhecidos automaticamente. Por exemplo: sites não autorizados, downloads que possam conter malwares.

Host	URI	Velocidade Atual	Velocidade Avaliada	Tamanho	Tempo
Estatísticas em tempo real para o servidor proxy 127.0.0.1:3128 (squid/3.1.18). Atualizar automaticamente em 15 segundos. [Atualizar] [Parar] Criado em : 13/03/2012 às 16:29:00.					
Total: 1 usuário(s) e 5 conexão(s) @ 0.00/0.00 KB/s (Atual/Avaliada)					
prinfoSeth					
	http://www.unidavi.edu.br/media/site/BotaoAutoAtendimento.pn ...			4 Kb	1s
	http://www.unidavi.edu.br/?pagina=FILE&id=66008			4 Kb	1s
	http://www.unidavi.edu.br/?pagina=FILE&id=66069			0 b	
	http://www.unidavi.edu.br/?pagina=FILE&id=65921			0 b	
	http://www.unidavi.edu.br/?pagina=FILE&id=52772			0 b	
Total:		0.00 KB/s	0.00 KB/s		
Total: 1 usuário(s) e 5 conexão(s) @ 0.00/0.00 KB/s (Atual/Avaliada)					
© SqStat 1.20 by Alex Samorukov, 2006 Tradução para Português (pt_BR) Marcio José - 2009					
[ Retornar ao WebAdmin ]					

**Figura 13:** SqStat.

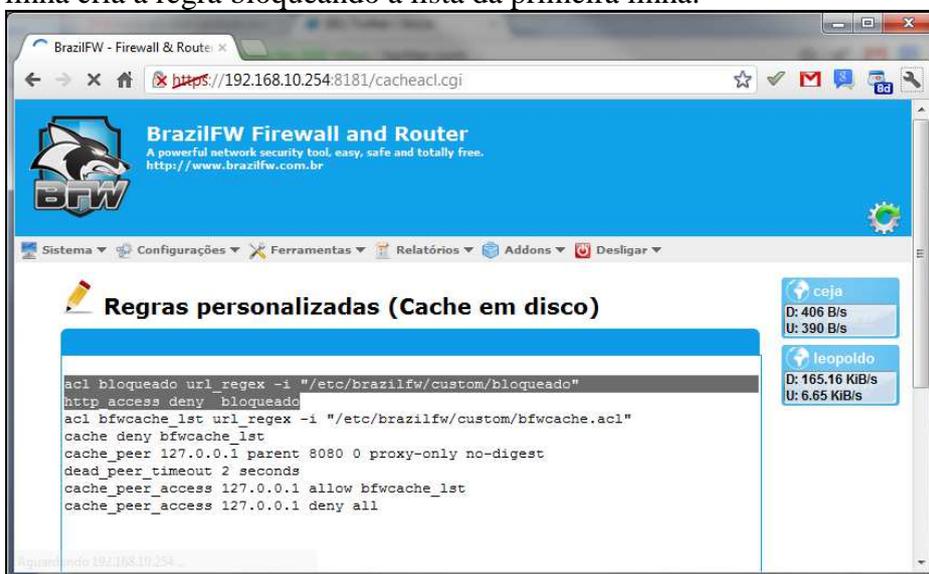
**Autor:** Acervo do autor.

A partir das observações dos dados da figura 12 e 13, o monitor<sup>4</sup> avalia a utilização de acesso as páginas web, e conforme as orientações dadas pelo NTE, direção da escola, são bloqueados os sites específicos, como por exemplo, sites pornográficos, redes sociais. Este bloqueio é feito através de uma configuração do serviço de Proxy Squid descrito na figura 14, via a inserção da URL completa ou parcial no arquivo denominado como “bloqueado” descrito na figura 15.

Na figura 14 foi personalizado a configuração do Proxy Squid através da inserção dos comandos nas regras personalizadas do Squid :

```
acl bloqueado url_regex -i "/etc/brazilfw/custom/bloqueado"
http_access deny bloqueado
```

Destas duas linhas, a primeira cria uma regra de uma lista de URL<sup>5</sup> e a segunda linha cria a regra bloqueando a lista da primeira linha.



**Figura 14:** O

Arquivo das regras personalizadas do Squid .

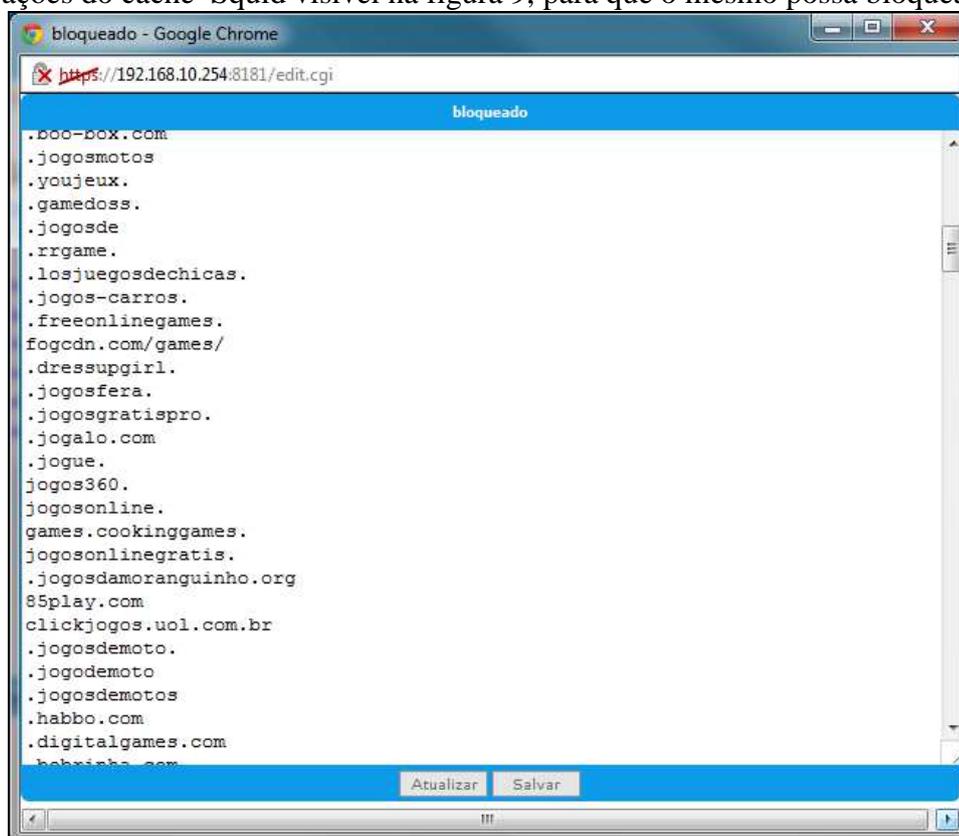
**Autor:** Acervo do autor.

<sup>4</sup> Professor Monitor: Professor com conhecimentos específicos em informática, contratado para cuidar da Sala de Tecnologia Educacional da escola e auxiliar os professores e alunos na mesma sala.

<sup>5</sup> URL : *Uniform Resource Locator* , em português *Localizador-Padrão de Recursos*, é o endereço de um recurso(um arquivo, uma impressora etc.), disponível em uma rede; seja a Internet, ou uma rede corporativa, uma intranet. Neste caso são os endereços das páginas web.



Na figura 15, um editor de texto assado via browser<sup>6</sup> é utilizado para inserir as URL no arquivo das URL bloqueadas, depois de salvar o arquivo, deve recarregar as configurações do cache Squid visível na figura 9, para que o mesmo possa bloquea-las



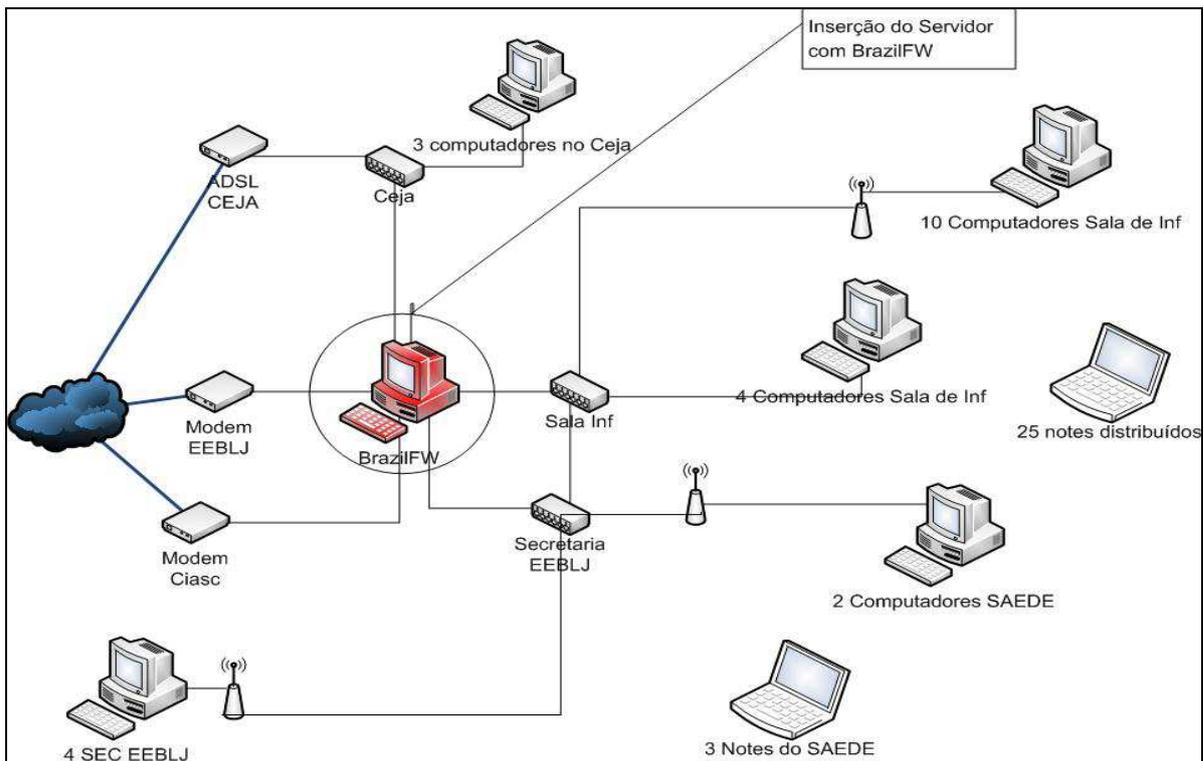
**Figura 15:** O Arquivo das regras personalizadas do Squid .

**Autor:** Acervo do autor

Na figura 16 observa-se a estrutura da rede reformulada as conexões físicas com a instalação do servidor com a distribuição Linux BrazilFW 3.0.256, neste novo layout o laboratório, secretaria, SAEDE, conexão wireless com os notes dos professores e alunos encontram o BrazilFW antes de das conexão com os links de internet, com a exceção do CEJA que usa a conexão direta com o modem/roteador ADSL.

---

<sup>6</sup> Browser : um programa utilizado para navegar páginas HTML como o Internet Explorer, Firefox, Chrome, outros.



**Figura 16:** Escopo EEBLJ com o servidor BrazilFW.

**Fonte:** Acervo do autor.

Ainda na figura 16, observam-se as duas conexões saindo do servidor com os switches da secretaria e o switch da sala de informática, e que os ambos estão se conectando também, isto se dá devido às conexões dos computadores se dividem em conexões lógicas, isto é, uma faixa ip para a secretaria e que se comunica com uma placa de rede do servidor, e outras duas faixa ips para outra placa de rede, uma para os equipamentos do laboratório, SAEDE e outra para uso geral como os notes dos professores e dos alunos com QOS separados.

## CONSIDERAÇÕES FINAIS

Em análise com a Escola objeto do estudo, viu-se que a necessidade da comunicação e aos acessos mundiais as redes públicas é necessitado cada vez mais, por isso no mercado existe uma variedade de ferramentas a serem implantadas para a solução de acesso e controle e a ferramenta apresentada / implantada nessa instituição ajudou e muito no desempenho e monitoramento do link existente, onde proporcionou uma facilidade a rede interna da escola.

A implantação da ferramenta BrasilFW, iniciou-se primeiramente com a configuração e a implantação de roteador / servidor<sup>7</sup> na sala de informática da escola, realizando um papel muito importante, porque é onde estão todas as máquinas do laboratório interligadas a um Hub / Switch que se comunicam entre si e assim passando para o acesso à internet. Assim atendendo o objetivo do artigo que é a comunicação dos computadores à rede de internet, com um ótimo monitoramento / controle e segurança.

Essa implantação viabilizou para o laboratório de informática a administração da rede interna e a constante disponibilização de acessos à rede mundial à Internet. Com isso

<sup>7</sup>Uma CPU com a distribuição Linux BrazilFW



visou-se maior produtividade com ênfase na aprendizagem, pois com os recursos disponíveis no BrazilFW foi possível bloquear os sites não autorizados definidos em conjunto pelo NTE de Taió, Direção da Escola e professor, conseguindo atender as necessidades e expectativas dos professores, dos Gestores da Escola de Educação Básica Leopoldo Jacobsen em relação ao desempenho e a utilização da rede.

## **REFERÊNCIAS**

- BISHOP, M. **Computer Security: Art and Science**. Addison Wesley, Boston, MA, 2003.
- BARKER, W. C., LEE, A. **Information Security – volume II: Appendices to guide for mapping types of information and information system to security categories**. NIST Special Publication 800-60, 2004.
- FÁVERI, Helena Justen de, BLOGOSLAWSKI, Ilson Paulo Ramos, FACHINI, Olimpio. **Educar para a Pesquisa: Normas para Produção de Textos Científicos**. 3ª Ed. Nova Letra, 2008.
- ISO. **Risk management – Vocabulary – Guidelines for use in standards**. ISO/IEC Guide 73:2002.
- ISO. **Common criteria for information technology security evaluation – part 1: Introduction and general model**. ISO/IEC 15408:2005.
- PFLEEGER, Charles P., PFLEEGER, Shari Lawrence. **Charles P. Pfleeger and Shari Lawrence Pfleeger: Security in Computing**. Prentice Hall, 2006.
- RODRIGUES, Diego. **Configurações de Segurança para o Firewall: Redes de Computadores**. Tec Portal, 2012.
- RODRIGUEZ, Martius V./ Ferrante, Augustin J. **CTecnologia de Informação e Gestão Empresarial**. Tradução Whashington Luiz Salles e Louse Anne N. Bonitzl, Rio de Janeiro: E-Papers, 2000.
- ROSS, Júlio. **Redes de Computadores**. Editora: Almeida e porto livros Técnicos Ltda., 2008.
- STONEBURNER, G., GOGUEN, A., FERINGA, A. **Risk management guide for information technology systems**. NIRT Special Publication 800-30, 2002.