

**Pontifícia Universidade Católica do Paraná – PUCPR**  
**Curso de Especialização – Redes e Segurança de Sistemas**

**Desenvolvimento de um Sistema Web para Gerenciamento de Usuários de  
uma LAN**

**Anderson Delafiori**

Contribuído com a montagem do ambiente, testes do sistema e na escrita e desenvolvimento do artigo.

Curitiba, fevereiro de 2013

# **Desenvolvimento de um Sistema Web para Gerenciamento de Usuários de uma LAN**

*Anderson Delafiori, Rafael da Silva Espíndola*

Especialização em Redes e Segurança de Sistemas  
Pontifícia Universidade Católica do Paraná

Curitiba, fevereiro de 2013

## **Resumo**

*A utilização da internet de maneira incorreta dentro do ambiente corporativo pode trazer imensos prejuízos financeiros e até jurídicos aos seus gestores, além da perda de produtividade da organização. A partir daí descobriu-se a necessidade em desenvolver uma maneira para controlar e monitorar todo e qualquer acesso à internet dentro das dependências da empresa e assim minimizar a possibilidade desses prejuízos acontecerem. O artigo descreve os passos da instalação e configuração de um sistema web para gerenciamento dos usuários de uma rede. O sistema interage com o Squid, o SARG, o IPFW, o Packet Filter e com o serviço de DHCP proporcionando um rígido controle do que cada usuário pode acessar e quando ele pode acessar, além de um monitoramento contínuo de suas ações.*

## **1. Introdução**

“O uso indiscriminado da Internet tem tirado o sono dos gestores de TI de diversas organizações. Por consequência, somam-se perdas em produtividade e segurança trazidas pelo acesso à Internet sem monitoramento no ambiente corporativo” [1].

A afirmação acima reflete a realidade de muitas empresas ao redor do mundo, pois o uso da Internet sem nenhum tipo de controle e monitoramento interfere diretamente na produtividade da empresa, gerando ainda uma grande insegurança as informações vitais da empresa que podem ser perdidas.

Além desses prejuízos a empresa ainda pode ser responsabilizada caso algum de seus funcionários infrinja a lei durante o exercício de seu trabalho, segundo o Art. 932 do Código Civil Brasileiro [2] e a Súmula 341 do Supremo Tribunal Federal [3]. Alguns dos principais crimes cometidos pela internet são: racismo, pedofilia, pirataria, violação de direitos autorais, *bulling*, ameaças, furtos e roubos.

Para uma correta utilização da Internet dentro de um ambiente corporativo, várias medidas são necessárias:

- Treinamento de todos os colaboradores
- Termo de uso e responsabilidades
- Mecanismo de controle de acesso
- Controle e monitoramento de usuários
- Relatório de logs

Este artigo irá focar na implementação de um sistema web, que irá interagir com o Squid, seu utilitário Sarg, IPFW, Packet Filter e o serviço de DHCP (*Dynamic Host Control Protocol*), os quais fornecem mecanismos de controle de acesso, monitoramento em tempo real das ações do usuário e relatório de logs; ficando como sugestão ao leitor a pesquisa de métodos de treinamento aos colaboradores e modelos de termo de uso e responsabilidades.

Durante a implementação cada funcionário terá seu usuário cadastrado no sistema com todas suas permissões e restrições, além do MAC Address de seu computador que será utilizado para autenticação.

O sistema de controle, juntamente com as outras ferramentas, será instalado sobre o sistema operacional FreeBSD 9.0 em um computador com duas interfaces de rede, uma para LAN e outra para WAN.

O FreeBSD foi escolhido porque é considerado um dos mais seguros e estáveis sistemas operacionais do mundo. O SO foi desenvolvido na Universidade de Berkeley que é responsável por todas as maiores tecnologias criadas e utilizadas na Internet, desde o primeiro servidor de correio eletrônico aos protocolos TCP/IP, DNS, entre outros. Além de ser considerado o Open Source mais organizado do mundo e atende diversos padrões de segurança, inclusive o POSIX.1E [4].

O sistema utiliza dois Firewalls, o primeiro é o IPFW (IPFirewall), o qual é nativo do FreeBSD, simples de configurar e muito flexível e o segundo é o PF (Packet Filter), portado do OpenBSD e considerado um dos mais seguros do mundo.

## **2. Descrição da Necessidade**

A empresa escolhida para utilização do sistema foi do setor de cerâmica de Sangão - Santa Catarina.

Os funcionários da empresa necessitam de um acesso à Internet para o cumprimento de suas funções, como por exemplo: acesso ao e-mail corporativo, determinadas páginas web e em determinados momentos MSN Messenger. Já seu proprietário precisa de um acesso livre a Internet e também de um meio de controlar e monitorar tudo o que seus funcionários acessam durante o horário de trabalho.

## **3. Ambiente**

A empresa possui uma infraestrutura de 19 computadores conectados a internet através de um link 100% dedicado com 1MB de velocidade, conforme a topologia abaixo.

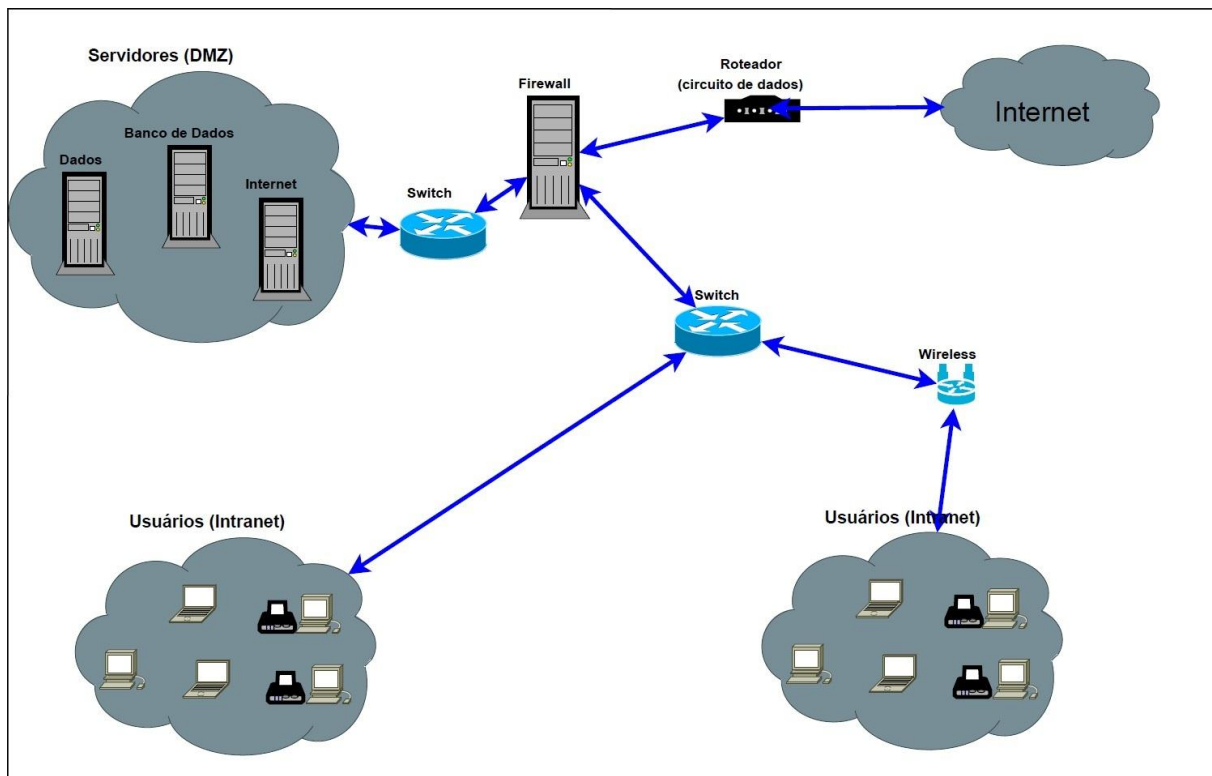


Figura 1 - Topologia de Rede da Empresa

A topologia de rede da empresa é composta por 4 (quatro) Servidores, 2 (dois) Switches, 1 (um) Modem Roteador e 1 (um) Roteador Wireless. Com exceção do Servidor Firewall, todos os outros são virtualizados e se encontram em uma DMZ (*Demilitarized Zone*, Rede Desmilitarizada).

Para utilização do sistema, o servidor (Firewall) precisa ser instalado entre o roteador e o Switch da empresa. No servidor a interface em0 (200.138.195.10/29) deve ser conectada no roteador e a em1 no Switch (192.168.2.254/24), sendo a configuração de rede efetuada no arquivo /etc/rc.conf:

```
## Configuração de Rede (/etc/rc.conf)
ifconfig_em0="200.138.195.10/29"
ifconfig_em1="192.168.2.254/24"
defaultrouter="200.138.195.9"
gateway_enable="YES"
hostname="firewall.empresatelhas.com.br"
```

#### 4. Solução Apresentada

A solução que será utilizada pela empresa, baseia-se em um software onde toda sua interface Web para entrada de dados, processamento e armazenamento foi desenvolvida em PHP.

##### 4.1 Instalação

Pré-requisitos para utilização do sistema:

- FreeBSD 9.0;
- Servidor Web (Ex: Apache, lighttpd);
- Suporte a PHP;
- Software SUDO, para executar comandos com privilégios pré-definidos;
- Kernel compilado com Firewall IPFW e PF;
- Proxy Squid;
- Software ISC-DHCP Server, para definir o endereçamento da rede.

Obs: Utilizado o PORTS para instalação dos softwares no FreeBSD [5].

How-to para implantação do sistema:

- O sistema deve ser colocado no diretório do servidor Web;
- O Software Sudo deve ser configurado para permitir alguns comandos específicos do usuário "www";
- Todos os outros softwares, tais como IPFW, PF e SQUID, necessitam de pequenas alterações além do padrão de cada administrador de rede, configurações simples;
- O recurso "net.link.ether.ipfw" deve estar ativado em /etc/sysctl.conf para controle da Camada 2 no Firewall IPFW;
- O diretório do sistema deve ser alterado para que o usuário e grupo "www" tenham permissão para modificações;
- Utilizar o sistema;

## 4.2 Scripts

### 4.2.1 Scripts Primários

```
#Arquivo Firewall IPFW
ipfw add allow layer2 src-ip 192.168.2.21 MAC any 5c:f9:dd:ed:dc:87 in via ${int_if}
keep-state #Rafael_Automação internet=Sim sites=Sim msn=Sim
#Arquivo DHCP
host Rafael_Automação { hardware ethernet 5c:f9:dd:ed:dc:87; fixed-address
192.168.2.21; default-lease-time 86400; max-lease-time 864000; }
```

### 4.2.2 Scripts Secundários

```
#Arquivo Firewall PF
192.168.2.21 #5c:f9:dd:ed:dc:87 Rafael_Automação
#Arquivo IPs sem restrição
192.168.2.21 #5c:f9:dd:ed:dc:87 Rafael_Automação
#Arquivo Liberados para MSN
192.168.2.21 #5c:f9:dd:ed:dc:87 Rafael_Automação
#Arquivo para gerenciamento de nomes dos funcionários
192.168.2.21 Rafael_Automação #5c:f9:dd:ed:dc:87
#Arquivo sites liberados integralmente e por período
globo.com
```

## 4.3 Descrição

A solução é simples e funcional, o foco é ter o controle sobre quem, onde e o que acessa. Todo novo equipamento conectado na rede precisa ser previamente cadastrado via web para que venha ter acesso garantido à internet. Neste processo o endereço IP atribuído é vinculado ao endereço físico (Mac Address), dificultando assim o acesso não permitido à rede

mundial de computadores. O administrador da rede também dispõe de mais dois recursos, o primeiro é a possibilidade de liberar ou não o mensageiro instantâneo da Microsoft, o Windows Live Messenger, o segundo é a liberação total ou não para acesso a websites.

## 5. Implementação e Utilização

Instalação do Sistema no Servidor.

Primeiramente o administrador da rede terá que acessar a parte de **network** do sistema para manutenção dos usuários (Adicionar, Alterar, Excluir) e definição dos tipos de serviço que cada um pode ou não acessar.

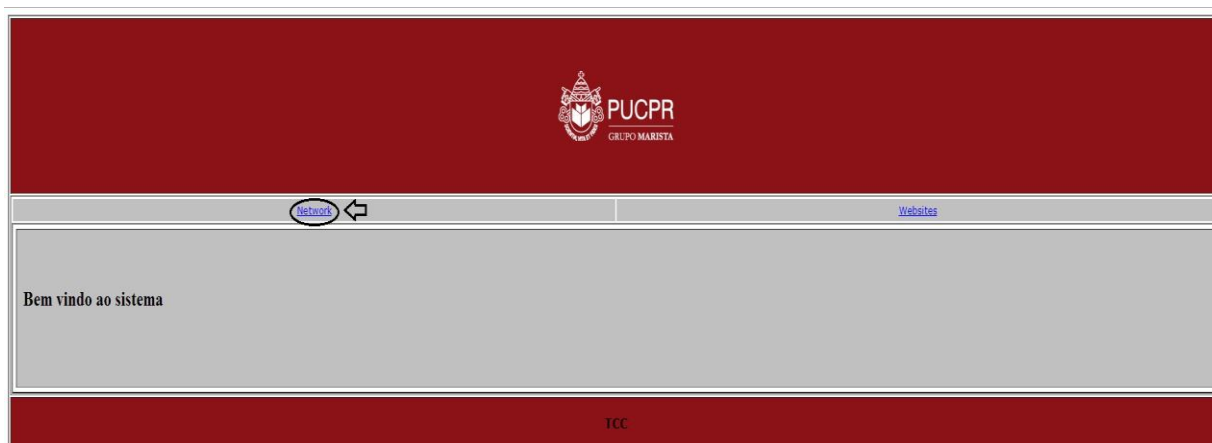


Figura 2- Tela de Acesso ao Sistema

### I. Adicionar

Ao adicionar um novo usuário as seguintes validações são realizadas:

- 1) Se o nome do usuário foi preenchido, caso contrário retorna um alerta.
- 2) Se o *Mac Address* foi preenchido, caso contrário retorna um alerta.
- 3) Se o IP foi preenchido, e também se a faixa de IP é a correta, caso contrário retorna um alerta.
- 4) Se o *Mac Address* já foi cadastrado anteriormente, caso contrário retorna um alerta.
- 5) Se o IP já foi cadastrado anteriormente, caso contrário retorna um alerta.

Feitas as validações necessárias, são feitas as inclusões das informações digitadas nos seguintes arquivos do tipo TXT:

- No arquivo do Firewall IPFW, exemplo:

```
ipfw add allow layer2 src-ip 192.168.2.21 MAC any 5c:f9:dd:ed:dc:87 in via ${int_if}
keep-state #Rafael_Automacao internet=Sim sites=Sim msn=Sim
```

- No arquivo do Firewall Packet Filter, exemplo:

```
192.168.2.21 #5c:f9:dd:ed:dc:87 Rafael_Automacao
```

- No arquivo do DHCP, exemplo:

```
host Rafael_Automacao { hardware ethernet 5c:f9:dd:ed:dc:87; fixed-address
192.168.2.21; default-lease-time 86400; max-lease-time 864000; }
```

- No arquivo do SARG, exemplo:

192.168.2.21 Rafael\_Automacao #5c:f9:dd:ed:dc:87

- No arquivo do Proxy Squid (referente ao MSN Messenger), exemplo:

192.168.2.21 #5c:f9:dd:ed:dc:87 Rafael\_Automacao

- No arquivo do Proxy Squid (referente aos usuários com acesso totalmente liberado), exemplo:

192.168.2.21 #5c:f9:dd:ed:dc:87 Rafael\_Automacao

- O Firewall IPFW, o Firewall Packet Filter, o Proxy Squid e o DHCP são recarregados.

## **II. Alterar**

Ao alterar a permissão de acesso dos itens "Internet", "Websites" e "Messenger", os seguintes processos são realizados:

- O sistema procura o MAC do usuário em todos os arquivos e a alteração é feita conforme a escolha do administrador de rede.
- O Firewall IPFW, o Firewall Packet Filter, o Proxy Squid e DHCP são recarregados.

## **III. Excluir**

Ao excluir um usuário, as seguintes ações são realizadas:

- O sistema procura a linha que possui o Mac do usuário em todos os arquivos e exclui.
- O Firewall IPFW, o Firewall Packet Filter, o Proxy Squid e DHCP são recarregados.

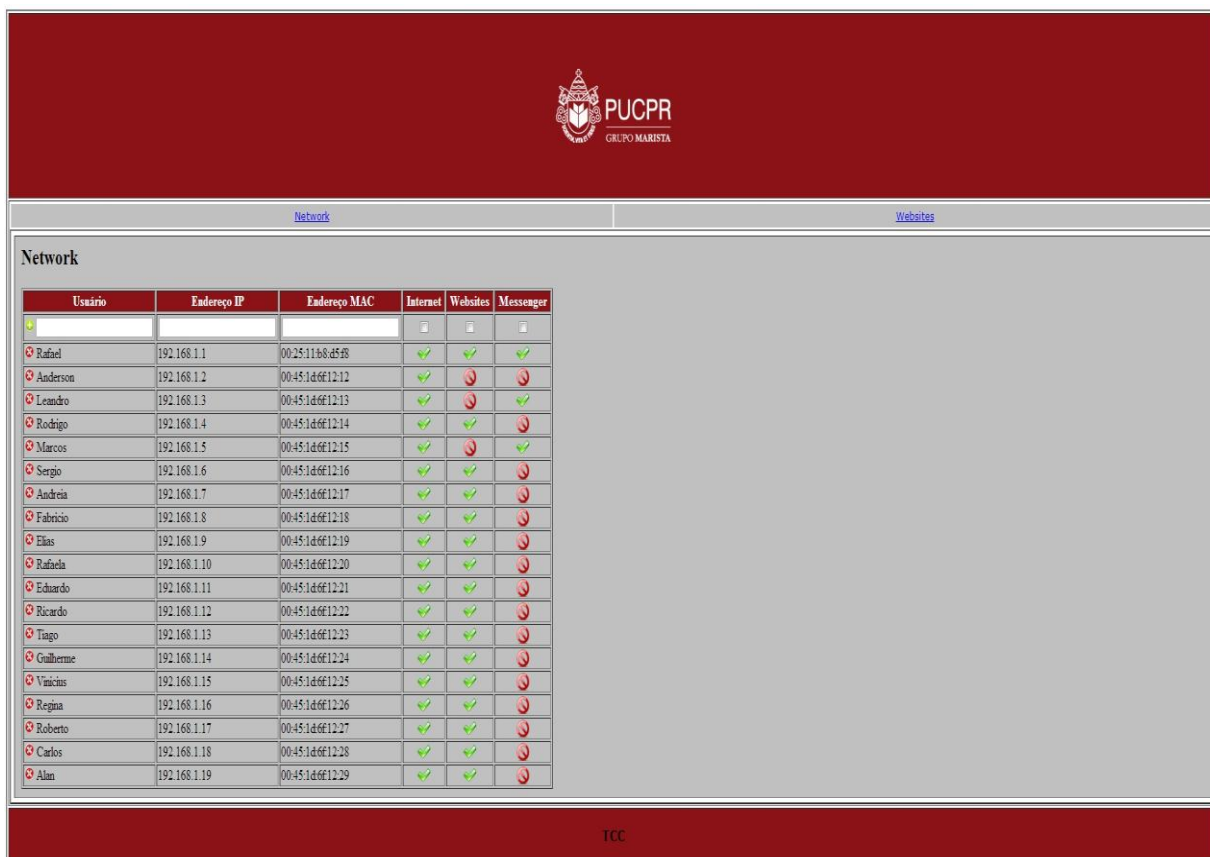


Figura 3 - Tela de Acesso ao Cadastro de Usuários

Após o cadastro do usuário é possível especificar quais websites os usuários poderão acessar integralmente ou somente por determinados períodos.

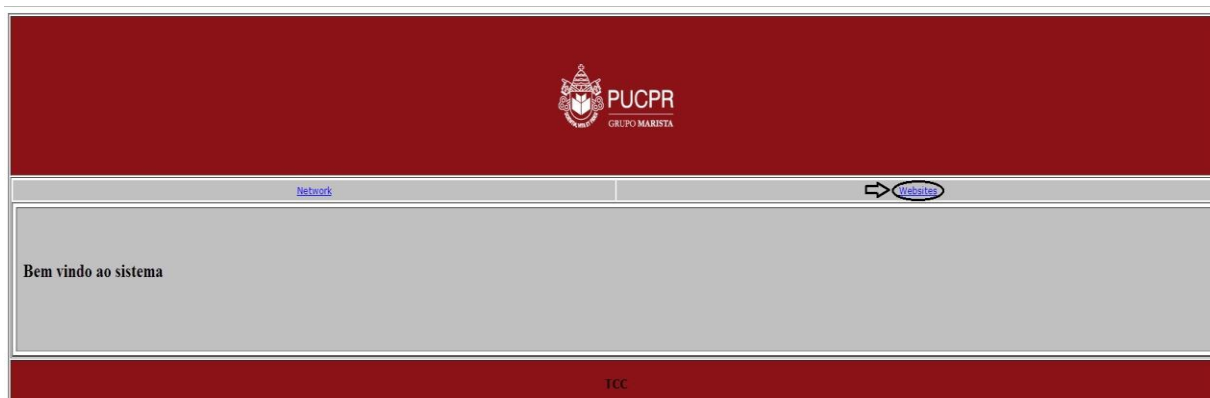


Figura 4 - Tela de Acesso ao Sistema

## I. Adicionar

Ao adicionar um novo website o sistema realiza as seguintes validações:

- 1) O sistema verifica se o site já existe, caso exista é retornado um alerta.
- 2) O sistema faz a busca no site adicionado pelos termos "http://" e "www.", caso encontre, eles são retirados.
- 3) Caso exista, o sistema também elimina toda a URL após o caractere "/", para que fique



organizado o cadastro de sites, por exemplo, ao cadastrar o site "http://www.pucpr.br/pesquisacientifica/mestradodoutorado.php", após todas as verificações e modificações ele ficará assim "pucpr.br".

- 4) Após o sistema obter exatamente o domínio a ser incluso, como por exemplo "pucpr.br", ele faz a checagem se o site já não foi cadastrado, caso esteja ele emite um alerta.

Após serem realizadas as validações necessárias, é feita a inclusão do website no arquivo do tipo TXT e o Proxy Squid é recarregado.

## II. Excluir

Ao excluir um website, as seguintes ações são realizadas:

- O sistema procura a linha que possui o Website no arquivo de sites e o exclui.
- O Proxy Squid é recarregado.

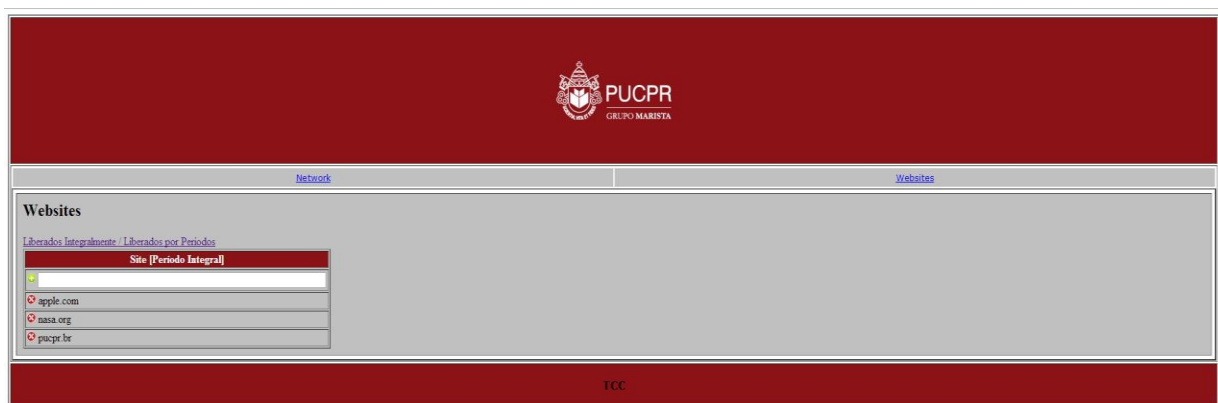


Figura 5 - Tela de Acesso ao Cadastro de Websites (Período Integral)

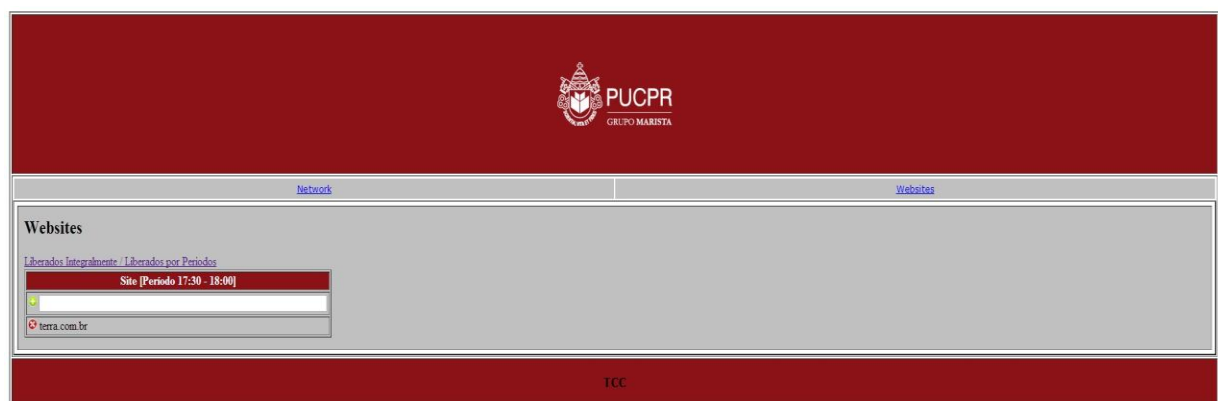


Figura 6 - Tela de Acesso ao Cadastro de Websites (Determinados Períodos)

## 6. Considerações Finais

A Internet tornou-se indispensável em qualquer ambiente corporativo mesmo tendo a possibilidade de trazer inúmeros problemas devido ao seu mau uso. Essa dependência da Internet pelas empresas ocorre devido criação de ferramentas de trabalho hospedadas na rede mundial de computadores (e-mail corporativo, *Web Services*, sistemas de gestão empresarial, entre outros) e da oportunidade de oferecer a cada dia que passa uma maior quantidade de serviços online a seus clientes.

Neste cenário em que riscos e necessidades caminham paralelamente, fica a cargo dos gestores e profissionais de TI a criação e implantação de políticas de acesso e mecanismos de controle que levem seus funcionários a compreender suas responsabilidades quando utilizam a internet no cumprimento de sua função.

Para alcançar um ambiente seguro e proporcionar o suporte a continuidade do negócio da organização, a empresa precisa utilizar em conjunto com o sistema que foi desenvolvido (ferramenta de controle e monitoramento dos usuários) uma boa política de segurança além de estar sempre conscientizando seus funcionários sobre os perigos do não cumprimento das normas de segurança.

## Bibliografia

- [1] Riscos, Controles e Legislação no uso da Internet nas Empresas. [http://www.sc.sucesu.org.br/pdf/cartilha\\_internet.zip](http://www.sc.sucesu.org.br/pdf/cartilha_internet.zip) – Acessado 12/12/2012
- [2] Código Civil Brasileiro – Artigo 927 ao Artigo 943. [http://www.dji.com.br/codigos/2002\\_lei\\_010406\\_cc/010406\\_2002\\_cc\\_0927\\_a\\_0943.htm](http://www.dji.com.br/codigos/2002_lei_010406_cc/010406_2002_cc_0927_a_0943.htm) - Acessado em 27/12/2012 – Acessado em 12/12/2012.
- [3] Súmula 341 – Supremo Tribunal Federal. <http://www.stf.jus.br/portal/jurisprudencia/listarJurisprudencia.asp?s1=341.NUME.%20NAO%20S.FLSV.&base=baseSumulas> - Acessado em 27/12/2012.
- [4] Por quê FreeBSD?. <http://www.freebsdbrasil.com.br/home.php?area=2&conteudo=5> – Acessado em 22/01/2013.
- [5] Pacotes e Ports: Adicionando programas no FreeBSD. [http://www.freebsd.org/doc/pt\\_BR.ISO8859-1/articles/linux-users/software.html](http://www.freebsd.org/doc/pt_BR.ISO8859-1/articles/linux-users/software.html) - Acessado em 22/01/2013.