UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

***CAMPUS* LUIZ MENEGHEL - CENTRO DE CIÊNCIAS TECNOLÓGICAS**

SISTEMAS DE INFORMAÇÃO

EDERSON MENDES VILELA

SISTEMA PARA GUARDA DE LOGS DE ACESSO BASEADO NO MARCO CIVIL DA INTERNET

Bandeirantes

2017

EDERSON MENDES VILELA

SISTEMA PARA GUARDA DE LOGS DE ACESSO BASEADO NO MARCO CIVIL DA INTERNET

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação e Licenciatura em Computação.

Orientador: Prof. Me. Wellington A. Della Mura

Bandeirantes

2017

EDERSON MENDES VILELA

SISTEMA PARA GUARDA DE LOGS DE ACESSO BASEADO NO MARCO CIVIL DA INTERNET

Projeto de Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito parcial para obtenção do grau de Bacharel em Sistemas de Informação e Licenciatura em Computação.

COMISSÃO EXAMINADORA

_____
Prof. Me. Wellington Aparecido Della Mura
UENP – *Campus* Luiz Meneghel

_____
Prof. Me. Carlos Eduardo Ribeiro
UENP – *Campus* Luiz Meneghel

_____
Prof. Me. Ricardo Gonçalves Coelho
UENP – *Campus* Luiz Meneghel

Bandeirantes, 05 de julho de 2017

RESUMO

O Marco Civil da Internet é a lei que regulamenta o uso da Internet no Brasil. O pilar da privacidade desta lei exige que provedores realizem a guarda do registro de acesso à *Internet* de seus usuários. A guarda dos registros deve ser realizada de forma confiável e permitir uma rápida consulta para a criação de relatórios de acesso. Diante desta necessidade, esse trabalho desenvolveu um sistema computacional que permite a uma organização, o gerenciamento e guarda dos registros de acesso de conexão de usuários. Os dados de acesso são armazenados em um banco de dados, considerando as diretrizes impostas pela lei do Marco civil da Internet. O sistema permite que as organizações realizem relatórios para análise desses registros quando possuir mais de um usuário conectado à rede. Para o desenvolvimento desse trabalho foi realizado o levantamento bibliográfico, levantamento dos requisitos baseado na lei do Marco Civil da Internet e o desenvolvimento do sistema.

Palavras-chave: Marco Civil da Internet. Registro de Acesso de Conexão. Privacidade.

ABSTRACT

The Brazilian Civil Rights Framework for the Internet is the law that regulates the use of Internet in Brazil. The privacy pillar of this law requires providers to carry out the custody of their users' Internet access registry. The log keeping must be performed reliably and allow quick queries for creating access reports. Given this need, this work aimed to develop a computer system that enables an organization the management and custody of users' access logs. The access data is stored in a database, taking into account the guidelines imposed by the current law. The created system allows organizations to create reports on these records when they have more than one user logged on to the network. For the development of this work, a bibliographic survey was carried out, a survey of the requirements based on the Internet Civil Law and the development of the system.

Keywords: Civil Internet Framework. Connection Access Log. Privacy.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ACL	(Access Control List) Lista de Controle de Acesso
CGI.BR	Comitê Gestor da Internet no Brasil
CSS	(Cascading Style Sheets) Folha de Estilo em Cascata
TCP	(Transmission Control Protocol) Protocolo de Controle de Transmissão
SARG	(Squid Analysis Report Generator) Gerador de Relatórios de Análise
DNS	(Domain Name System) Sistema de Nomes de Domínio
FTP	(File Transfer Protocol) Protocolo de Transferência de Arquivos)
IP	(Internet Protocol) Protocolo de Internet
NAT	(Network Address Translation) Tradutor de Endereços de Rede
MVC	(Model-View-Control) Controle de Exibição do Modelo
SGDB	Sistema Gerenciador de Banco de Dados
SARG	Squid Analysis Report Generator
ACLs	(Access Control List) Lista de Controle de Acesso
ISP	(Internet Service Provider) Provedor de Serviço Internet

SUMÁRIO

1. INTRODUÇÃO

A Internet no Brasil surgiu aproximadamente ao final da década de 80 por intermédio das Universidades brasileiras, visando o compartilhamento de suas informações com o Estados Unidos. Foi a partir de 1989 que a Internet ganhou força em meio ao surgimento da Rede Nacional de Ensino e Pesquisa (RNP).

No período de 1997 foram criadas as redes locais de conexão distribuídas, possibilitando o acesso em qualquer território nacional. E em 2011, conforme divulgados os dados do Ministério da Ciência e Tecnologia, quase 80% das pessoas já possuíam acesso à Internet, que se refere a aproximadamente 60 milhões de computadores conectados (História, 2016).

Com o crescimento exponencial de acesso de usuários e provedores de serviços da Internet no Brasil, surge uma lei de regulamentação dos direitos e deveres dos usuários e provedores de serviços da Internet. O Marco Civil da Internet, que segundo Cgi.br (2013) é a regulamentação do uso da *Internet* no Brasil. A lei foi aprovada pela Câmara de Deputados em 25 de março de 2014, e pelo Senado Federal em 23 de abril de 2014 e sendo sancionada pela presidente Dilma Rousseff, sendo caracterizada oficialmente de Lei Nº 12.965/14.

A lei Nº 12.965/14 define regras para o uso da Internet no Brasil por meio da previsão de princípios garantias, direitos e deveres para quem usa a rede (Internet).

Conforme Cgi.br (2013) a lei do Marco Civil da Internet se baseia em 3 pilares, que visam garantir a integridade do usuário no uso da rede: neutralidade, privacidade dos usuários e a liberdade de expressão.

Segundo o Cgi.br (2013) o pilar de Privacidade da Lei Nº 12.965/14 define que os provedores de Internet serão responsáveis por armazenar e disponibilizar os registros de conexão e de acesso de seus usuários na Internet. O pilar de Privacidade ainda ressalva que a disponibilização desses registros de conexão será feito somente por meio de ordem judicial.

Neste contexto, o pilar de Privacidade do marco civil com suas diretrizes atinge todas as empresas que possuem mais de um colaborador com acesso à Internet, no requisito de identificar a origem do acesso.

1.1 FORMULAÇÃO DO PROBLEMA

Com a definição da lei do Marco Civil da Internet em seu pilar de privacidade, que os registros de conexão dos usuários poderão ser solicitados mediante a ordem judicial, para identificação da origem do acesso. Cria-se a dificuldade para empresas e organizações quando notificadas judicialmente, em realizar a identificar do usuário que realizou o acesso.

1.2 OBJETIVOS

Os objetivos desse Trabalho de Conclusão de Curso estão divididos em um objetivo geral e cinco objetivos específicos.

1.2.1 Objetivo Geral

Este trabalho tem como objetivo geral desenvolver um sistema, que possibilite a emissão de relatórios de acessos dos usuários à *Internet,* tendo como base as diretrizes impostas pelo Marco Civil da Internet.

Com essa ferramenta será possível gerenciar e armazenar os registros de conexão dos usuários em um banco de dados. Com os dados armazenados será possível adequar empresas de pequeno e médio porte em relação as diretrizes impostas pelo Marco Civil da Internet em seu pilar de privacidade.

1.2.2 Objetivos Específicos

Os objetivos específicos são:

- Definir os objetivos impostos pela lei do Marco Civil da Internet no requisito de guarda dos registros de acesso à Internet dos usuários;

- Definir os requisitos e fazer a análise do sistema proposto;
- Implementar o sistema com base nos arquivos de log do servidor *Proxy Squid*;
- Realizar um comparativo da ferramenta desenvolvida nesse trabalho com ferramentas similares.
- Validar a ferramenta através de simulações de requisição de ordem judicial na solicitação dos registros de conexão.

1.3 JUSTIFICATIVA

O Marco Civil da Internet conforme Cgi.br (2013), foi constituído para quem utiliza a Internet no Brasil, ditando normas e diretrizes para seu uso. A lei prevê que os dados referentes aos registros de conexões e acesso de informações, deverão ser guardados pelos provedores de Internet. O chamado “registro de conexão”, que segundo a lei é o “conjunto de informações referentes para identificação do terminal utilizado para o envio e recebimento dos pacotes de dados”.

Com a exigência da lei em seu Art. 10, § 1º, de que provedores de Internet realizem o armazenamento dos registros de conexões de seus usuários e que em seu Art 13, § 1º, de que a responsabilidade pelo armazenamento dos registros não poderá ser transferida a terceiros, cria-se a necessidade das organizações de realizar o armazenamento dos registros de seus usuários, quando possuir mais de um usuário conectado à Internet.

Desta forma, foi desenvolvido nesse trabalho um sistema que possibilite armazenar os registros de conexão dos usuários em um banco de dados e disponibilizar relatórios desses registros, possibilitando sua aplicação em organizações de pequeno e médio porte.

Essas empresas quando notificadas judicialmente ou forem alvo de investigação, poderão identificar o colaborador responsável pelo o acesso que originou conteúdo ou acesso alvo de ação criminal, eximindo a organização de qualquer acusação.

1.4 ORGANIZAÇÃO DO TRABALHO

Este trabalho está organizado na forma descrita a seguir:

- No capítulo 2 é apresentada a fundamentação teórica;
- No capítulo 3 é apresentado o projeto desenvolvido;
- Por fim, no capítulo 4 é apresentada a conclusão;

2. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão apresentadas as fundamentações teóricas de modo que se obtenha capacitação para um melhor entendimento acerca do tema proposto neste trabalho.

Por se tratar do desenvolvimento de uma ferramenta para guarda dos registros de acesso de usuários à Internet, serão abordados tópicos referentes ao desenvolvimento da ferramenta.

Para o desenvolvimento deste trabalho foi abordado definições sobre o assunto, softwares relacionados com a ferramenta, trabalhos relacionados já desenvolvidos, o Marco Civil da Internet entre outros.

2.1 Marco Civil da Internet

O Marco Civil da Internet oficialmente chamado de Lei N° 12.965/14. Conforme a Presidência da República (2014), o Marco Civil da Internet é uma lei sancionada que regulamenta o uso da Internet no Brasil. A lei consolida por meio da previsão os direitos, princípios e deveres voltados para quem usa a rede e o desenvolvimento da Internet no Brasil.

O surgimento do projeto do Marco Civil da Internet se iniciou em 2009 e foi aprovado na Câmara dos deputados em 25 de março de 2014, e pelo senado federal. Sua aprovação e publicação ocorreu em 23 de abril de 2014, sendo sancionado logo depois pela então presidente Dilma Rousseff descrito pelo Presidência da República (2014).

Conforme informado pelo site Cgi.br (2013) “a iniciativa partiu da percepção de que o processo de expansão do uso da Internet por um crescente número de pessoas colocou novas questões e desafios relativos à proteção dos direitos civis e políticos dos cidadãos”. Com isso foi de extrema importância a imposição de diretrizes para o futuro da Internet, para base de um uso livre e aberto, mais também que permitisse os avanços tecnológicos e o desenvolvimento econômico e político (CGI.BR, 2013).

A proposta se iniciou de uma disposição da Secretaria Legislativas do Ministério da Justiça e em parceria com o Centro de Tecnologia da Fundação Getúlio

Vargas no Rio de Janeiro, foi estabelecido a formulação de um marco civil brasileiro para uso da Internet. Tendo como base a Resolução de 2009 do Comitê Gestor da Internet no Brasil denominada “Os princípios para a governança e uso da Internet” (Resolução CGI.br/RES/2009/003/P).

Com a iniciativa da instituição do Marco Civil da Internet, tendo que seus princípios definidos pelo CGI.br, ganhou repercussão internacional. Conduziu o Brasil a ocupar uma posição destaque com sua criação regulatória que garante princípios na Internet e métricas para proteção de seus usuários (CGI.BR, 2013).

2.1.1 Privacidade do Marco Civil da Internet

Segundo Cgi.br (2013) “a privacidade é um direito fundamental do homem, presente na Declaração Universal dos Direitos Humanos das Nações Unidas e assegurado pela Constituição Federal brasileira”, que está definida em seu artigo 5º, incisos X e XII, o qual se refere a resguardar a inviolabilidade da intimidade, da vida privada e protege o sigilo da correspondência, telegráficas e telefônicas, salvo somente por ordem judicial.

Para Cgi.br (2013) a privacidade refere-se à proteção das informações que diz respeita ao cidadão, tanto no sentido do seu direito de estar só ou resguardando sua privacidade de espaço e vida íntima. A quebra da privacidade pode gerar, além de tudo, constrangimentos políticos e pessoais, discriminação social, econômica, étnica, religiosa entre outros. Neste sentido o pilar de Privacidade evita a utilização de dados de terceiros sem seu prevê consentimento, evitando investigações indevidas.

O Marco Civil da Internet trata de itens importantes relacionados à privacidade dos usuários. Em seu artigo 10º da lei Nº 12.965, "que um provedor não pode violar o direito à intimidade e vida privada dos seus usuários, ou seja, não pode divulgar seus dados ou ainda monitorar os dados trafegados". No seu artigo 11º lei Nº 12.965, refere-se que "o monitoramento e armazenamento desses dados podem ser feitos desde que o provedor receba ordem judicial com esta instrução". O tempo de armazenamento dos dados, que anteriormente era de dois anos, atualmente é de no máximo um ano.

2.1.2 Neutralidade do Marco Civil da Internet

A neutralidade da rede corresponde que todos os conteúdos e usuários sejam tratados da mesma maneira, sem que haja interferência de conteúdo ou distinção de pacotes pelo seu destino na rede. Conforme o Cgi.br (2013) “a neutralidade de rede é básica em qualquer interação social e um princípio embutido na origem da Internet”.

Exemplificando, as empresas de telecomunicações, podem ofertar diversos pacotes de serviços de banda, mais não bloquear ou limitar velocidade do serviço contratado para conteúdo ou aplicativos específicos. Como define Cgi.br (2013) “diferenciar por tipo de serviço ou de usuário, o que pode ou não ser acessado, eliminando a possibilidade de escolha de empresas e pessoas na Internet, é uma quebra inadmissível da neutralidade”.

Na lei Nº 12.965 em seu artigo 9º, do Marco Civil da Internet, refere-se ao responsável pela transmissão e serviço de telecomunicações utilizados. “O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço terminal ou aplicativo” (PRESIDÊNCIA DA REPÚBLICA, 2014), que visa garantir os direitos da neutralidade de rede.

2.1.3 Liberdade de Expressão do Marco Civil da Internet

O termo “inimputabilidade” aplicado à Internet, que trata da insuficiência do sujeito de responder por sua conduta delituosa. Assim, a inimputabilidade é causa da retirada da culpa. Para o Cgi.br (2013), “a jurisprudência sobre responsabilização de atos delituosos de pessoas no uso da Internet relacionados a conteúdos disponibilizados em sítios, redes sociais, blogs, etc. mostra que é necessário o estabelecimento de parâmetros para o julgamento de tais processos”.

No artigo 15º da lei Nº 12.965, defini as obrigações dos prestadores de serviços de telecomunicações. Conforme Presidência da República (2014) “prestadores de serviços de conexão à Internet e prestadores de serviços/aplicações e prestadores de serviços de hospedagem de páginas web não podem ser responsabilizados civilmente por danos decorrentes de conteúdos gerados por terceiros”.

O artigo de inimputabilidade da rede, existente nos “Princípios para a

governança e uso da Internet", conforme Cgi.br (2013) "o combate a ilícitos deve atingir especificamente os responsáveis finais, aqueles que de fato cometeram o crime, e não aqueles que operam os meios utilizados para uso da Internet".

2.2 Regulamentação da Internet em Diversos Países

Enquanto este mundo novo da Internet cresce a cada dia, em contrapartida, o conceito de "dados" se intensifica no contexto globalizado, bem como a discussão sobre o uso justo e a necessidade de conscientização sobre os efeitos da tecnologia na rotina das pessoas. Um dos maiores desafios continua sendo a compreensão do potencial do ciberespaço.

A Internet não se limita a espaços geográficos, tradições nacionais entre outras. Portanto, o crescimento desta interação de informações, pode acarretar violações de direitos que normalmente auxiliem nas relações sociais e comerciais. Isso significa uma carência de se encontrar um sistema jurídico de influência mundial, suficiente para atender, administrar e solucionar questões da rede.

A falta de um sistema mundial que jurisdicione a rede no mundo faz com que países como o Brasil e diversos países no mundo criem leis e decretos para regulamentação do uso da Internet. Alguns países se tornaram marcos para outros países no mundo com a implantação de diretrizes que regulamenta o uso da Internet, como o Brasil com a implantação da lei do Marco Civil da Internet.

2.2.1 Lei de Neutralidade na Rede no Chile

O Chile criou a lei nº. 20453, que garante a neutralidade da Internet, sendo o primeiro país do mundo a aprovar uma importante lei que garanta a neutralidade da rede. A lei foi aprovada no congresso e publicada em agosto de 2010 pelo deputado Gonzalo Arenas, precursor da iniciativa.

A neutralidade da lei define que os provedores de acesso não poderão bloquear, discriminar, interferir nem restringir os direitos de nenhum usuário no uso da Internet. Segundo Dias (2010) "Os provedores deverão oferecer um serviço que não distinga arbitrariamente conteúdos, aplicações ou serviços".

Como no Brasil, no Chile a neutralidade na rede resulta que os provedores não possam interferir nos conteúdos que são acessados pelos usuários, e Dias (2010) define os principais pontos que garanta a neutralidade da rede, que são:

- Os ISP (aqueles que prestam acesso à Internet) estão proibidos de interferir, discriminar ou entorpecer de qualquer forma os conteúdos, aplicações ou serviços, salvo ações destinadas a garantir a privacidade dos usuários, a proteção contra vírus e a segurança da rede.
- Os ISP devem fornecer serviços de controle parental.
- O serviço deve fornecer ao cliente uma série de dados que permitam identificar corretamente o que está sendo contratado.
- A segurança da rede e a privacidade dos usuários deve ser preservada acima de tudo.
- Garantia de acesso a todo tipo de conteúdo, serviços ou aplicações disponíveis na rede sem nenhuma distinção da fonte de origem ou da propriedade destes.
- É terminantemente proibida atividades que restrinjam a liberdade dos usuários para o uso de conteúdo ou serviços, salvo expressa petição dos usuários.

A neutralidade da lei, busca garantir aos usuários, que não sejam impostas restrições ou limitações por provedores de Internet ou serviços, que conforme Dias (2010) são os que controlam de uma forma ou outra o uso e o trafego de toda a rede.

2.2.2 Regulamentação de Serviços e Comércios Eletrônicos da Espanha

Segundo Brasil e Cultura (2010) a Espanha sancionou a Lei 34/2002 que define diretrizes para serviços da sociedade da informação e o comércio eletrônico e a Lei 25/2017, que impõe deveres para a conservação dos dados relacionados à comunicação eletrônica e de redes públicas de comunicação, sendo os dois principais reguladores sobre a governança da Internet.

De acordo com Brasil e Cultura (2010) “a lei 25/2007 obriga aos prestadores de serviços de comunicações eletrônicas disponíveis ao público ou aos exploradores de redes públicas de comunicação a conservar dados”. Para uso da Internet, os dados a serem armazenados para identificação do usuário são: nome; endereço da rede; e Protocolo de Internet.

Para a identificação do usuário, a lei especifica os seguintes dados, descritos a seguir por Brasil e Cultura (2010):

• Dados de destino;

• Dados para determinar data, hora e local da comunicação;

• Dados para identificar o tipo de comunicação;

• O equipamento de comunicação;

• A localização do equipamento.

Com as obrigações criadas pela lei espanhola, não será permitido navegação anônimo na Internet, quando acessada por meio de redes públicas.

Para o armazenamento dos dados conforme a lei 25/2007, os dados deveram ser resguardados por 12 meses, sendo possível ser prorrogado até 24 meses. Os dados somente poderão ser fornecidos ou divulgados mediante ordem judicial.

Ainda fica definido pela lei, que os órgãos e agentes autorizados a realizar a solicitação dos dados, que são segundo (BRASIL; CULTURA, 2010):

• Membros das Forças e Corpos de Segurança;

• Funcionários da Direção de Vigilância Alfandegária;

• Funcionários do Centro Nacional de Inteligência.

Em relação responsabilidade dos provedores, publicação de artigos de terceiros, Brasil e Cultura (2010) “a lei 34/2002, em seu artigo 16, determina que os prestadores de serviço não serão responsáveis pela informação armazenada sempre que não tenham conhecimento que a informação é ilícita ou que lesione bens ou direitos de terceiros”. Quando reconhecido o conteúdo ilícito, os provedores deveram com rapidez remover ou impedir o acesso ao conteúdo.

2.2.3 Regulamentação da Internet na Itália

A lei determina que os registros de conexão devem ser mantidos armazenados pelos provedores de Internet por um determinado tempo prescrito pela lei. Na contratação do serviço o usuário deve ter previa consciência desses parâmetros. Em conformidade com Brasil e Cultura (2010) os provedores de Internet ficaram obrigados de conservar os logs de acesso à Internet dos usuários pelo prazo determinado pela lei, e no ato da subscrição do contrato os provedores deveram dar previa ciência aos seus usuários dessa determinação.

No que se refere ao armazenamento dos registros estabelecido na legislação, em conformidade com Cultura e Pesquisa (2010) “é estabelecido que o provedor conserve por 12 meses os dados telemáticos (Internet) e por 24 meses os dados telefônicos. Os provedores disponibilizarão os dados de navegação armazenados às autoridades policiais, desde que a solicitação seja formalizada por via judicial”.

Para Cultura e Pesquisa (2010) “a atual legislação exige a identificação do usuário, o provedor de Internet poderá eximir-se de responsabilidades penal ou civil, ou limitar sua responsabilidade, mediante a comprovação da autoria do conteúdo publicado”.

E Cultura e Pesquisa (2010) complementa que não poderá ser realizado o acesso à Internet de forma anônima. Sendo possível o uso de apelidos e pseudônimos. Sendo o provedor de Internet, por sua vez, conseguir realizar a identificação do usuário. Mais para efeito, é de total importância no ato da efetivação do contrato de serviço que seja apresentado documentos de identificação válidos.

Ainda consta no decreto-lei nº 190 (16/08/2005) segundo Cultura e Pesquisa (2010) “é oportuno ressaltar a obrigatoriedade, por parte dos gestores de pontos públicos de Internet (“cybercafé”), da identificação dos usuários de serviços, por meio do arquivamento de fotocópia do documento de identidade apresentado”.

2.3 Gerência de Redes

Com o aumento significativo dos computadores no ambiente de trabalho, as redes de computadores se tornam indispensáveis para realização das atividades rotineiras das empresas, se tornando não mais uma infraestrutura dispensável.

Com este cenário que surgiu o termo gerência de rede, que para McCabe (2017) pode ser definida como uma série de atividades e monitoramentos de meios físicos ou lógicos em uma rede, com a finalidade de assegurar confiabilidade, tempos de respostas aceitáveis e segurança das informações, buscando aumentar sua eficácia e produtividade.

Essa série de atividades consistem em um conjunto de ações, que segundo McCabe (2007) são: controlar; planejar; alocar; implantar; coordenar e monitorar recursos de uma rede. Com a gerência de rede bem estruturada definida pode-se garantir o sucesso de qualquer rede.

As redes de computadores são formadas por dois componentes, que são Hardware e Software conforme Kurose e Keith (2006), que trabalham em conjunto garantindo seu funcionamento e desempenho. Deve-se ter uma boa gerência entre esses componentes afim de garantir o perfeito funcionamento.

A gerência de rede pode ser dívida em cinco camadas, que são: Negócio; Serviço; Rede; Ativos de rede e Dispositivos segundo McCabe (2007), como

demonstrado na Figura 1 - Hierarquia das camadas de Gerência de Rede descrito a seguir:

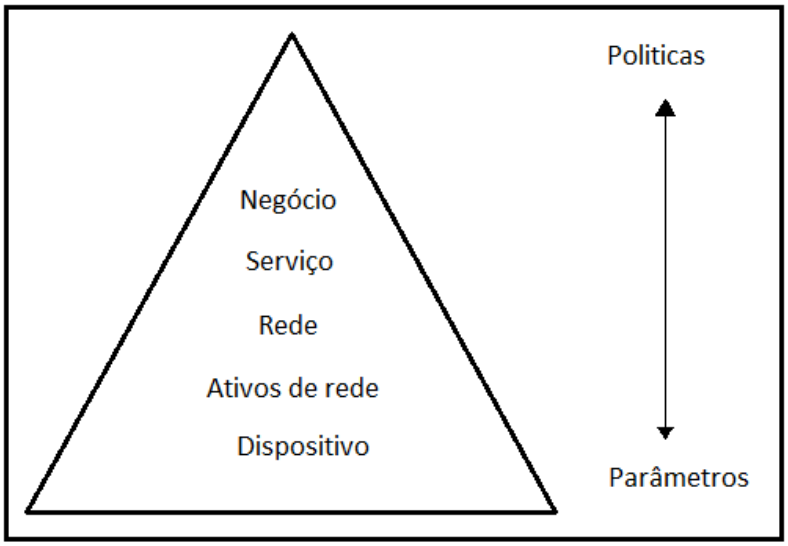


Figura 1 - Hierarquia das camadas de Gerência de Rede
Fonte: Adaptado de McCabe (2007)

Está representada no início a camada mais abstrata da topologia da hierarquia, a camada de gerência de negócio que terá suas características mediante a atividade de negócio da empresa, e a mais específica, a camada de gerência de dispositivo no final que se refere a infraestrutura utilizada.

Para esse trabalho foi abordado as duas primeiras camadas da Hierarquia de McCabe (camada de negócio e camada de serviço). O sistema desenvolvido neste trabalho permite que o usuário gere relatórios dos registros de conexão dos usuários (camada de gerência de negócio) por meio de uma aplicação Web (camada de gerência de serviço).

Com a adoção da gerência de rede foi possível obter um controle das atividades e no monitoramento das ações ocorrentes nos recursos da rede sendo em Software e Hardwares. Com a coletar das informações da rede, foi possível uma análise destas informações e definir a solução para problema.

2.4 Servidor Proxy

Serviço de proxy pode ser definido como um software que trabalha entre um cliente e o serviço solicitado na Internet, o proxy interpreta as solicitações do cliente e encaminha ao seu servidor de destino a requisição feita pelo cliente.

Para Lunardi (2005) “servidor ou serviço de proxy é um software que localiza hosts na Internet, buscando as informações solicitadas através de requisições”.

A seguir, é descrito na Figura 2 – Serviço de Proxy como é um servidor de Proxy de acordo com Lunardi (2005). Que nada mais é, que um cliente se conecta ao servidor de proxy, em seguida, solicita uma requisição, o servidor oculta o IP do solicitante e busca na rede a requisição, e após realizar a busca devolve a requisição para cliente requisitante.

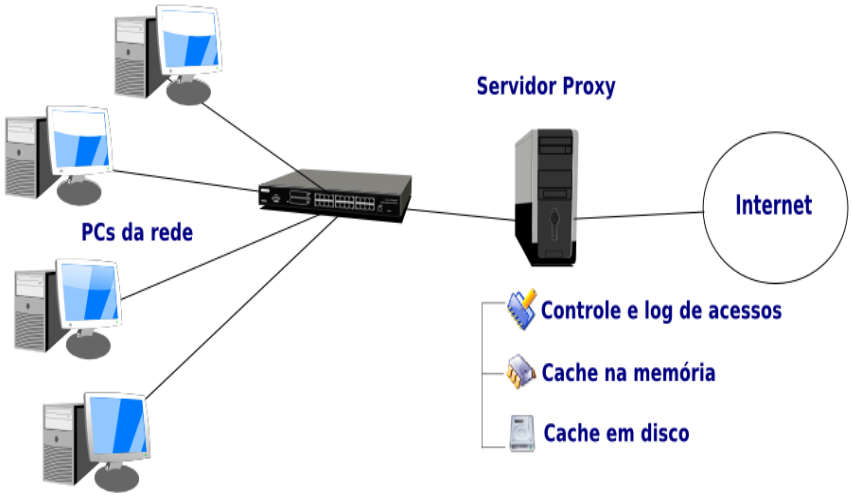


Figura 2 – Serviço de *Proxy*

Fonte: Lunard (2005)

O proxy possui quatro tipos fundamentais que são Proxy Web, Proxy cache, Proxy Reverter e Proxy Transparente. Alguns desses servidores de proxies possuem várias funções, tais como Web e cache ou reverter e cache (PONTES; HIRATA; HONÓRIO, 2016).

Um servidor de Proxy conforme Ricci Mendonça (2006) pode ser usado para quatro propósitos básicos, descrito a seguir:

- Aumento na velocidade de resposta das aquisições: com o armazenamento de cache de um servidor de proxy, possibilita o armazenamento em memória das requisições mais recentes, e disponibiliza esse conteúdo armazenado de forma eficiente e com economia de banda quando uma nova requisição for solicitada.
- Compartilhamento de conexão de Internet: Em uma rede local, as

máquinas não possuem endereços de IPs válidos para navegação direta na Internet. Com o servidor de Proxy, as máquinas solicitam as requisições para o servidor de Proxy, e o mesmo acessa a Internet com um IP válido satisfazendo as requisições solicitadas.

- Controle de acesso: O servidor de Proxy possibilita realizar um controle de acesso à Internet por meio de ACLs (*Access Control List*), gerenciando e controlando os usuários da rede por meio de um controle de permissões e restrições.
- Relatórios de acesso: É realizado o armazenamento dos registros de acessos dos usuários no formato de log, que permite ao administrador do servidor o acesso aos relatórios de navegação.

O serviço de proxy-cache faz um redirecionamento das portas solicitadas pelos seus usuários, uma vez que as solicitações são realizadas via porta 80 e são redirecionados à porta 3128.

2.5 Cache

Conforme Macêdo (2016) o servidor de Proxy Cache permite que seja realizado o armazenamento de páginas requisitadas de um servidor Web com mais frequência. Quando é solicita uma requisição de um site pelo usuário a uma página de um servidor Web, o Proxy armazena uma cópia do conteúdo em cache no próprio servidor e sua data.

Quando o usuário faz uma requisição de uma página a um servidor Web, essa requisição passará pelo servidor de Proxy, que irá verificar se a requisição já se encontra em cache na máquina, que por sua vez se encontrar em cache buscará a data da página remota, e verifica se a data da página é mais atual a que se encontra em cache, se não for é fornecida para o cliente a página em cache, sem a necessidade de realizar o download novamente da página solicitada.

Em questão de armazenamento em cache Macêdo (2016) fala “existe um limite dado pelo administrador da rede para que ele não armazene tudo”. O armazenamento do cache terá um limite, ao atingir esse limite o cache irá apagar as páginas mais antigas, que para Macêdo (2016) “ele apagará os documentos mais antigos, ou seja, aqueles que raramente são acessados, deixando, assim, os sites

mais visitados”.

O cache aumenta muito o desempenho do acesso das requisições para as páginas Web, sendo que o acesso é no próprio cache (local), o que é mais rápido que o acesso via Internet como ilustra a Figura 3 - Proxy Cache:

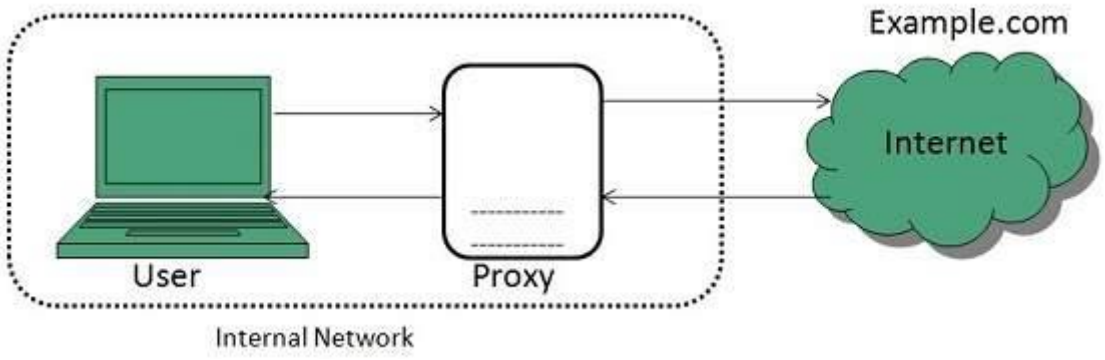


Figura 3 - Proxy Cache
Fonte: Tutorials Point (2016)

2.6 Squid

O Squid é uma ferramenta para administração de acesso, muito utilizável por administradores que têm diariamente grandes volumes de acessos à Internet, que possuem banda saturada com requisições a sites não relacionados à finalidade, e possibilita definir listas de bloqueios para restrições dos acessos sem finalidade.

Com o Squid você pode instalar um servidor Linux, e fazer com que outras máquinas clientes acessem páginas Web e sites FTP por meio do servidor Linux, as máquinas clientes precisam somente estar com os seus (gateway) padrões apontados para o servidor Proxy.

Wessels (2004) descreve esse fluxo de usuários passando pelo servidor Squid exemplificado na Figura 4 – Servidor Proxy Squid a seguir:

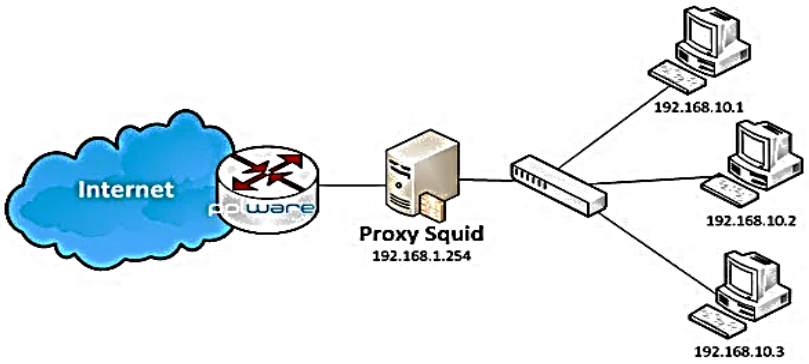


Figura 4 – Servidor Proxy Squid
Fonte: Adaptado de Wessels (2004)

Na figura é apresentado os clientes conectados a uma rede juntamente com o serviço de proxy do Squid em um servidor Linux. Os clientes solicitam ao serviço de proxy do Squid as páginas que desejam acessar, o servidor recebe essa requisição e busca na Internet essa solicitação, após devolve ao cliente solicitante a requisição encontrada.

Segundo Wessels (2004) "o Squid é um servidor de proxy de código-fonte aberto onde seu projeto iniciou-se em 1996 e utilizou-se como base o código-fonte do software Harvest cache Project".

Wessels (2004) ressalta ainda que o Squid é um servidor Proxy bastante popular, e enfatiza alguns dos seus principais usos:

- Economia de banda do provedor de Internet enquanto se navega na Web;
- Diminui o tempo que uma página leva para carregar;
- Possibilidade de coleta estatística sobre o tráfico Web da rede;
- Bloqueio de acesso dos usuários a páginas inapropriadas conforme a política de uso da empresa;
- Garantia de que apenas usuário autorizados possam navegar na Internet.

O Squid possui suporte para vários protocolos como HTTP, HTTPS, FTP. Ele é um Proxy com cache de alta desempenho para clientes web, simplificando, ele é um servidor Proxy utilizado para acelerar a navegação dos usuários de sua rede pela web” (LUNARDI 2005).

Segundo Lunard (2005) “Ele caracteriza-se por ser um *software* especializado, que faz operação de Proxy de Web e FTP, livre e com um ótimo suporte para servidores Linux”.

2.6.1 Ferramentas de Análise de Logs do Squid

Para Orso (2006) “com uso de ferramentas auxiliares, é possível analisar uma instalação e os resultados obtidos dos logs do Squid, possibilitando acompanhamento e refinamento da configuração”.

A análise de Logs pode-se ser realizada hoje através de várias ferramentas já disponíveis. Possuindo uma variedade de analisadores de Logs, Orso (2006) descreve duas ferramentas para análise dos logs baseadas no Squid, que são elas:

- O Calamaris: Esta ferramenta permite a criação de relatórios estatísticos em vários formatos, por exemplo HTML e TXT, a geração de relatórios não somente para controle de acesso por meio do Squid, mas também para outras ferramentas, entre elas: Proxy Server, Oops, Netcache, Novell Internet Caching System, e outros. Sua plataforma é em Perl, não existe a necessidade de compilação para o uso.
- O Sarg: É uma ferramenta desenvolvida em C, por um brasileiro, que autoriza acompanhamento através de relatórios os sites acessados. Os relatórios gerados pelo SARG são completos e de simples compreensão para o que se propõem, eles ainda apresentam informações como total de trafegados, conexões, bytes, data e horário de acesso e identifica se a requisição foi realizada ou negado. Disponível hoje em mais de 18 idiomas, entre eles o Português, sendo em principais distribuições Linux parte integrante e sendo visto como principal ferramenta de análise de logs do Squid.

Além das ferramentas descritas por Orso (2006), pode-se encontrar mais três ferramentas descritas por Conceição (2012) em seu trabalho, sendo elas:

- O Free-sa: O Free-sa é uma ferramenta para análise de registro de acessos do Squid bastante similar ao SARG. Entre suas principais diferenças em relação ao SARG é sua performance, maior velocidade de relatórios e um maior suporte aos padrões HTML da W3C (World Wide

Web Consortium) nos relatórios gerados no formato HTML.

- Redline Internet Access Monitor: O Redline Internet Access Monitor é uma ferramenta comercial para monitorar a eficiência do uso da banda de Internet por parte dos funcionários de uma empresa. A ferramenta permite a visualização de quais usuários estão utilizando mais a Internet, o que cada usuário está acessando, além também de observar quanto tempo que o usuário gasta na navegação. Além disso a ferramenta suporta diversos proxys, dentre eles o Squid.
- Firewall Analyzer: o Firewall Analyzer é uma ferramenta de gerência de rede para análise de logs de dispositivos de segurança de redes. A ferramenta é útil para análise de logs do firewall da rede, possibilitando assim a detecção de falhas de segurança como tráfego de vírus, ataques entre outros. Além disso, também é possível analisar outros itens, como o uso de banda da rede, possibilitando identificar o perfil do uso do tráfego da rede, além de monitorar a navegação web dos usuários da rede.

3. PROJETO

Neste tópico será apresentado a arquitetura do sistema proposto para desenvolvimento, tendo como foco principal a análise dos requisitos do sistema para atingir seus objetivos. O foco desse tópico não é a tecnologia a ser utilizada, e sim identificar e detalhar as funcionalidade e requisitos. Os artefatos gerados nesse tópico auxiliaram no entendimento da regra de negócio do sistema, compreensão de suas funcionalidades e seus objetivos.

3.1 METODOLOGIA

Para realização desse trabalho foi empregada a metodologia baseada na pesquisa exploratória em busca de conhecimento teórico fundamentado em livros, revistas, artigos, periódicos, artigos científicos, publicações cientificas e páginas web. O intuito dessa pesquisa é a aquisição de novos conhecimentos para o desenvolvimento desse trabalho e a obtenção de um cenário para um estudo de ambiente real. Assim, o objeto de estudo de caso é a análise de um servidor de *Proxy* proveniente da Universidade Estadual do Norte do Paraná (UENP).

O estudo de caso real foi feito com base nos logs de um servidor de Proxy da UENP, priorizando propósitos acadêmicos, com o intuito de analisar o fluxo de requisições de acesso à Internet pelos acadêmicos. Com isso será possível coletar os registros de acesso à rede mundial de computadores com o uso da ferramenta *Squid*.

O trabalho foi desenvolvido para pequenas e médias empresas e organizações que desejam se adequar aos requisitos imposto pela lei do Marco Civil da Internet em seu pilar de Privacidade.

A metodologia do trabalho consistiu em:

- Pesquisas Bibliográficas: Foi realizado estudos em livros, tutoriais, publicações e artigos aos quais contribuíram no aperfeiçoamento do conhecimento em relação às ferramentas que foram utilizadas para o desenvolvimento do sistema;
- Foi adotada a metodologia de desenvolvimento Incremental;
- Levantamento de requisitos: Foi levantado por meio de estudos e análise, os requisitos necessários para o desenvolvimento desse sistema;
- Implementação e aplicação do sistema proposto.

3.2 Arquivo de Log

Os logs de acesso dos usuários foram registrados e capturados por meio software neste trabalho. O software utilizado foi o Proxy Squid, tendo em vista o padrão e as informações que se utiliza para geração de seu relatório de log.

As informações que o Squid gera em seu relatório são: Time; Elapsed; Client Address; Code/Status; Bytes; Method; URL; Server IP Address; Username e Mime Type. Essas informações que o Squid gera em seu relatório são correspondentes as exigências que a lei do Marco Civil da Internet impõe para a identificação do usuário e a guarda dos registros de log.

A seguir um exemplo do formato das informações do relatório de log do Squid, e a descrições dessas informações conforme Tabela 1 – **Descrição dos dados de log do Squid** para um melhor entendimento:

1334159203.532 168 192.168.0.140 TCP_MISS/200 3718 GET http://fotos.vrum.com.br/patio/MG/469990/199164010_1tn.jpg - DIRECT/200.188.178.49 image/jpeg

Tabela 1 – Descrição dos dados de log do Squid

Time: 1334159203.532	Data e Hora em que foi feita a requisição do usuário
Elapsed: 168	Tempo em segundo em que a solicitação demorou
Client Address: 192.168.0.140	IP do usuário que fez a solicitação
Code / Status: TCP_MISS/200	Ação que o proxy tomou Código / Status
Bytes: 3718	Tamanho da requisição em Bytes
Method: GET	Método em que foi usado: GET, POST, PUT e etc
URL: http://fotos.vrum.com.br/patio/MG/469990/199164010_1tn.jpg	URL completa da requisição
Server IP Address: DIRECT/200.188.178.49	Status da hierarquia do Squid / Endereço de IP do servidor da requisição
User name	Nome do usuário que realizou a requisição
Mime Type: image/jpeg	Tipo do arquivo

3.3 Estratégias de Desenvolvimento

O sistema tem como base de interação com os usuários, a plataforma de desenvolvimento Web. O acesso é realizado por meio da Internet, minimizando custos com investimento e equipamentos para implantação, possibilitando o acesso de forma heterogenia a partir de qualquer sistema operacional.

O processo de desenvolvimento do sistema foi dividido em dois módulos, o módulo de Interface com o usuário, responsável por toda a interação que o sistema possui com o usuário, como telas, imagens e relatórios e o módulo de extração de dados, que será responsável pela extração e armazenamento dos dados no sistema.

Na Figura 5 – Módulos do Sistema, é ilustrada a representação da divisão dos módulos utilizados para o desenvolvimento do sistema.

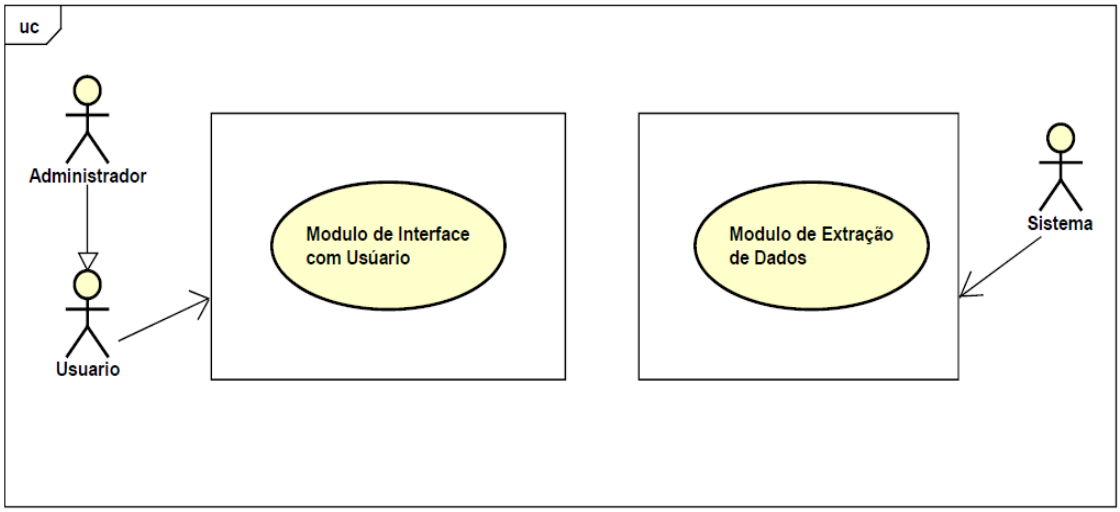


Figura 5 – Módulos do Sistema

Módulo de extração de dados: responsável pela leitura, extração e gravação dos dados no banco de dados MongoDB, dos registros de acesso do arquivo de log do Proxy.

Esse módulo será executado automaticamente pelo Cron do sistema em um horário pré-determinado. Quando executado, ele abrirá o arquivo de log do Squid e fará a leitura dos dados, em seguida irá armazenar esses dados no banco de dados MongoDB, como ilustrada na Figura 6 – Fluxograma de Extração de dados.

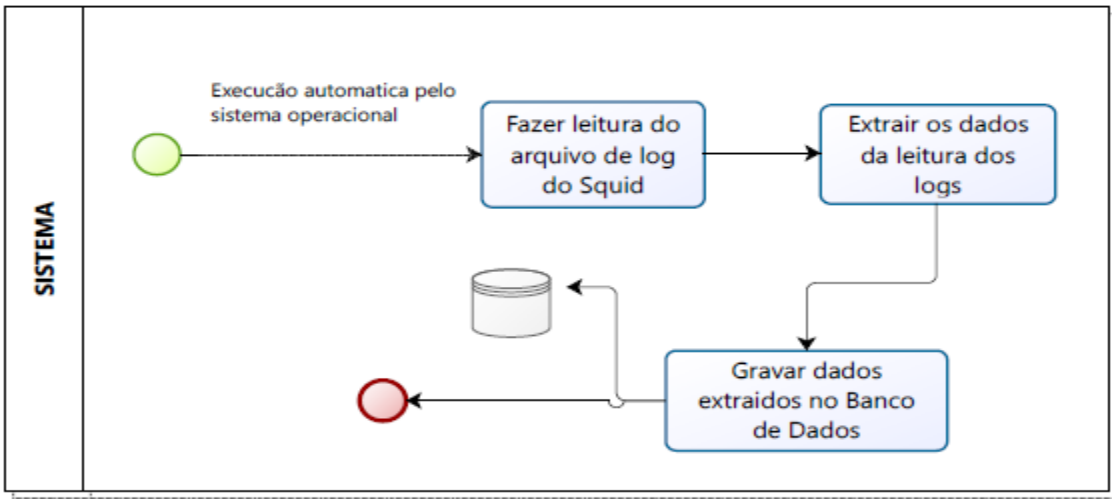


Figura 6 – Fluxograma de Extração de dados

Para armazenamento dos registros de conexão o sistema segue uma Scheme no banco de dados MongoDB. O Scheme desenvolvido para o banco de dados MongoDB pode ser visto a seguir na Figura 7 - Scheme MongoDB

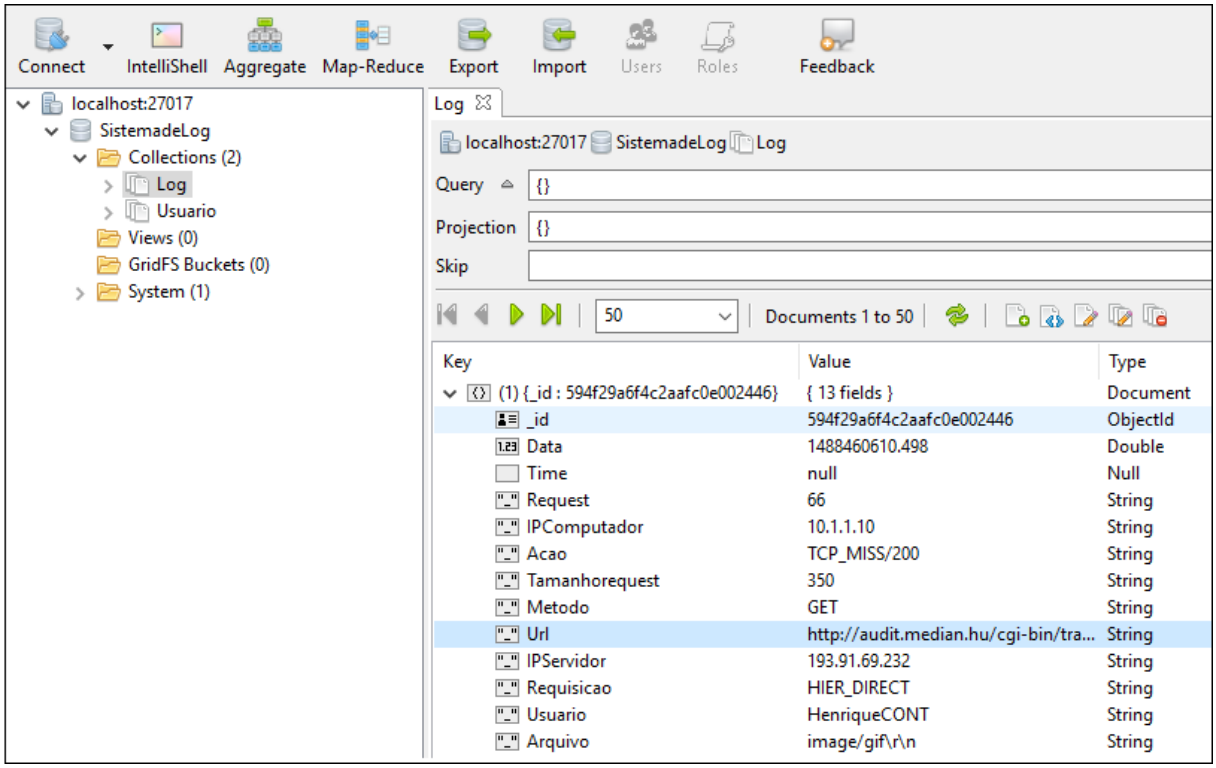


Figura 7 - Scheme MongoDB

<u>Módulo de interface com usuário</u>: responsável pelo armazenamento das páginas utilizadas para interação e a manipulação do usuário com o sistema.

O acesso aos dados desse módulo é dado através de permissão de acesso de usuário. Para o usuário acessar os dados desse módulo deverá abrir o sistema e

informar o nome e senha de usuário, após o sistema validar o acesso do usuário será direcionado a tela inicial do sistema no qual terá acesso aos recursos, como ilustrada na Figura 8 – Fluxograma do módulo de interface.

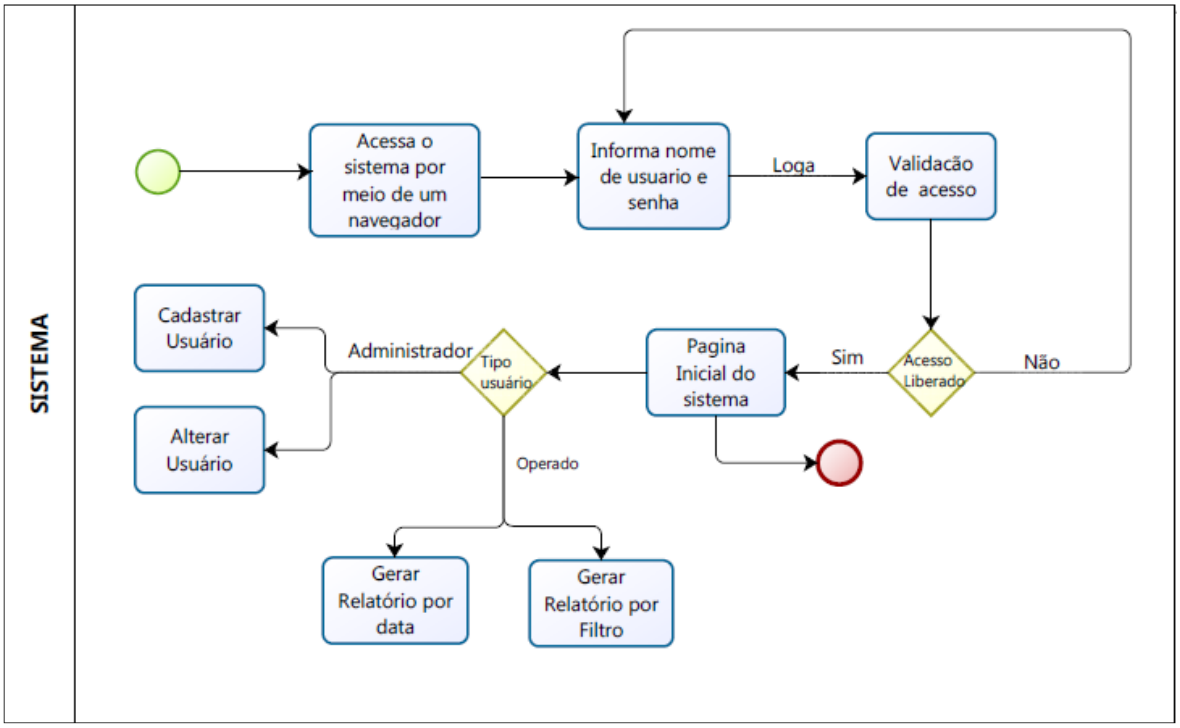


Figura 8 – Fluxograma do módulo de interface

3.4 Identificação dos Requisitos

A identificação dos requisitos se deu por meio das funcionalidades do sistema desenvolvido, na compreensão de seu domínio de aplicação. No levantamento dos requisitos foram identificados a necessidade do sistema para exercer suas funcionalidades, tanto no contexto de desempenho quanto de funcionalidade.

Os requisitos tende a ser alguns mais importantes que outros, para melhor entendimento desses requisitos, foram divididos e classificados como requisitos funcionais e requisitos não funcionais, e definido as regras de negócio descritos a seguir:

Requisitos funcionais

Com as funcionalidades desenvolvidas nesse projeto foi possível identificar os seguintes requisitos funcionais:

Tabela 2 – Tipos de Usuários

Identificador	RF001	**Categoria**	Funcionalidade

Nome	Tipos de Usuários		
Versão	1	**Prioridade**	Essencial
Descrição	O sistema deverá possuir dois tipos de usuário: usuário e administrador.		

Tabela 3 – Acesso ao Sistema

Identificador	RF002	**Categoria**	Funcionalidade
Nome	Acesso ao Sistema		
Versão	1	**Prioridade**	Essencial
Descrição	O usuário e o administrador deverão realizar autenticação para acessar o sistema.		

Tabela 4 – Permissão de Acesso 01

Identificador	RF003	**Categoria**	Funcionalidade
Nome	Permissão de Acesso 01		
Versão	1	**Prioridade**	Essencial
Descrição	O administrador poderá gerenciar os usuários (cadastrar, alterar, excluir).		

Tabela 5 – Permissão de Acesso 02

Identificador	RF004	**Categoria**	Funcionalidade
Nome	Permissão de Acesso 02		
Versão	1	**Prioridade**	Essencial
Descrição	O administrador terá acesso a todas as funcionalidades do sistema.		

Tabela 6 - Permissão de Acesso 03

Identificador	RF005	**Categoria**	Funcionalidade

Nome	Permissão de Acesso 03		
Versão	1	**Prioridade**	Essencial
Descrição	O usuário terá acesso somente a sua conta e os relatórios.		

Tabela 7 - Permissão de Acesso 04

Identificador	RF006	**Categoria**	Funcionalidade
Nome	Permissão de Acesso 04		
Versão	1	**Prioridade**	Essencial
Descrição	O usuário poderá alterar sua conta.		

Tabela 8 – Relatório por Data

Identificador	RF007	**Categoria**	Funcionalidade
Nome	Relatório por Data		
Versão	1	**Prioridade**	Essencial
Descrição	O sistema deverá possibilitar relatório por data.		

Tabela 9 – Relatório por Filtro

Identificador	RF008	**Categoria**	Funcionalidade
Nome	Relatório por Filtro		
Versão	1	**Prioridade**	Essencial
Descrição	O sistema deverá possibilitar relatório por filtro.		

Tabela 10 – Descrição do Relatório por Filtros

Identificador	RF009	**Categoria**	Funcionalidade
Nome	Descrição do Relatório por Filtro		

Versão	1	**Prioridade**	Essencial
Descrição	O relatório por filtro deve permitir que o usuário ou administrador selecione as opções que deseja como data inicial, data final, site, identificação do usuário, ordenação de pesquisa, período de tempo e atributos de pesquisa.		

Tabela 11 – Descrição do Relatório por Data

Identificador	RF010	**Categoria**	Funcionalidade
Nome	Descrição do Relatório por Data		
Versão	1	**Prioridade**	Importante
Descrição	O relatório por data deverá possuir somente a data inicial, data final da pesquisa e a opção de selecionar usuário, e deverá retorna à identificação do usuário, o site acessado e a data de acesso.		

Requisitos não funcionais:

Os requisitos não funcionais foram identificados visando o desempenho e a segurança desejável que o sistema deverá possuir:

Tabela 12 – Acesso ao Sistema

Identificador	RNF001	**Categoria**	Acesso
Nome	Acesso ao sistema		
Versão	1	**Prioridade**	Essencial
Descrição	O acesso ao sistema somente se dará por meio de autenticação		

Tabela 13 – Armazenamento de Senha

Identificador	RNF002	**Categoria**	Armazenamento
Nome	Armazenamento de Senha		

Versão	1	**Prioridade**	Importante
Descrição	O armazenamento da senha no banco de dados do sistema deverá ser criptografado.		

Tabela 14 – Frequência de Disponibilidade

Identificador	RNF003	**Categoria**	Disponibilidade
Nome	Frequência de disponibilidade		
Versão	1	**Prioridade**	Importante
Descrição	O sistema deverá estar disponível 24 horas por dia e 30 dias por mês.		

Tabela 15 – Design da Interface

Identificador	RNF004	**Categoria**	Usabilidade
Nome	Design da interface		
Versão	1	**Prioridade**	Importante
Descrição	O sistema deverá ser desenvolvido para rodar em ambiente web, e sua interface deve ser de fácil entendimento pelo usuário.		

Tabela 16 – Resposta do Sistema

Identificador	RNF005	**Categoria**	Desempenho
Nome	Resposta do sistema		
Versão	1	**Prioridade**	Importante
Descrição	O sistema deverá possuir um tempo de resposta aceitável para com as requisições e carregamento das páginas, podendo variar dependendo da rede.		

3.5 Modelo de Caso de Uso

Os modelos de caso de uso ilustram e descrevem a execução das atividades de cada membro do sistema permitindo visualizar suas reponsabilidades, identificando as interações de sequência de trabalho que poderão realizar em relação as suas tarefas com os demais integrantes.

Com os casos de usos é possível representar a interação entre os membros envolvidos com o sistema, ilustrando suas associações com atores para com suas funcionalidades.

O caso de uso para esse sistema foi elaborado pensando nos cenários que envolve cada membro do sistema com suas atuações, tarefa ou funcionalidade e a ralação entre elas.

Na Figura 9 – Diagrama de Caso de Uso é apresentado os casos de uso do sistema:

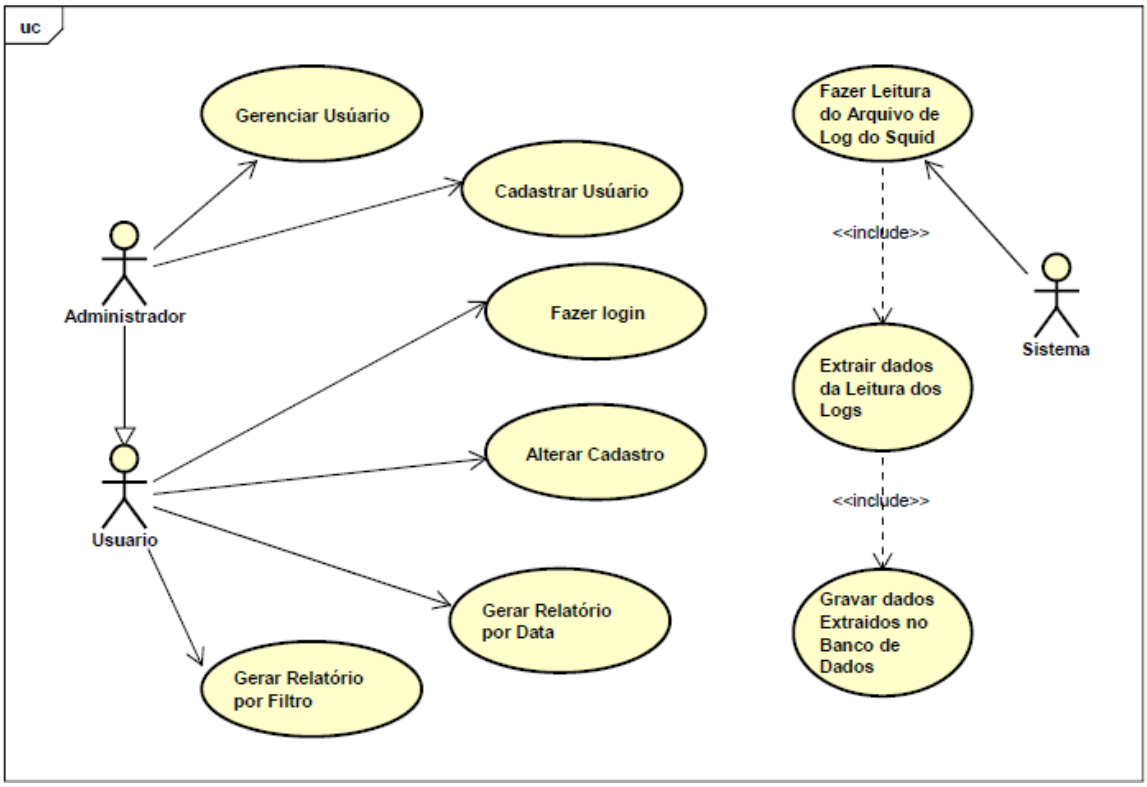


Figura 9 – Diagrama de Caso de Uso

A Figura representa os nove casos de uso existente no sistema, sendo seis casos de usos de interação com os usuários e três de interação com o sistema. O administrador terá total acesso os casos de uso e o usuário só terá acesso aos casos

de uso Fazer Login, Alterar Cadastro, Gerar Relatório por Data e Gerar Relatório por Filtro.

O sistema possui três casos de uso que os usuários do sistema não terão acesso, sendo eles: Fazer Leitura do Arquivo de Log do Squid, Extração dos Dados da leitura dos Logs e Gravar dados Extraídos no Banco de Dados.

Esses casos de usos serão executados pelo próprio sistema, por meio do Cron do Linux. O CronTab possibilita realizar configurações para executar aplicações em um horário pré-determinado, deste modo possibilitando a execução da aplicação sem a necessidade de intervenção externa.

3.6 Diagrama de Classes

A representação da estrutura de relação entre os objetos e suas associações será representada pelo diagrama de classe. O diagrama de classes representará de forma abstrata os elementos que representaram o conjunto de objetos do sistema a ser desenvolvido, assim como suas características, atributos e métodos.

O diagrama de classe representa a interação dos objetos e conceitua a representação de domínio do projeto. Com o diagrama demostra-se as especificações principais com reação a interação com a interface da arquitetura, e seus principais métodos para implementação. Desta forma possibilitando a visualização dos detalhes para desenvolvimento, tais como descrição dos recursos, detalhamento de atributos e modelo utilizado como guia no desenvolvimento do sistema.

Para melhor visualização do diagrama de classe, foi modelado o diagrama de classe, que contempla as classes especificadas no desenvolvimento do sistema. A representação do diagrama de classe é ilustrada na

Figura 10 – Diagrama **de Classe** demostrados a seguir:

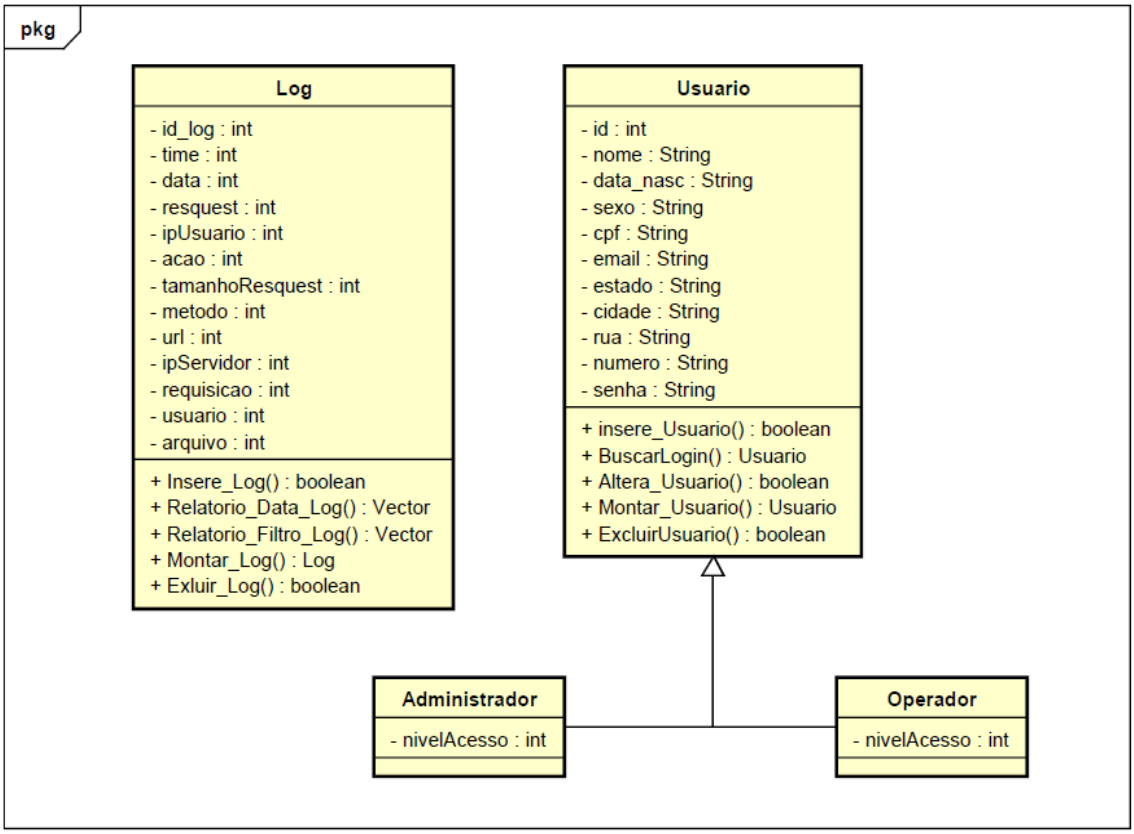


Figura 10 – Diagrama de Classe

3.7 Diagrama de Pacotes

A divisão por pacotes facilita a manutenção o entendimento da transição entre as classes. No desenvolvimento do sistema, sua organização se deu por meio de pacotes, facilitando o entendimento do código, e a localização das referidas classes utilizadas no desenvolvimento. Os pacotes estão divididos da seguinte forma, conforme demostrada na

Figura 11 - Diagrama **de Pacotes** a seguir:

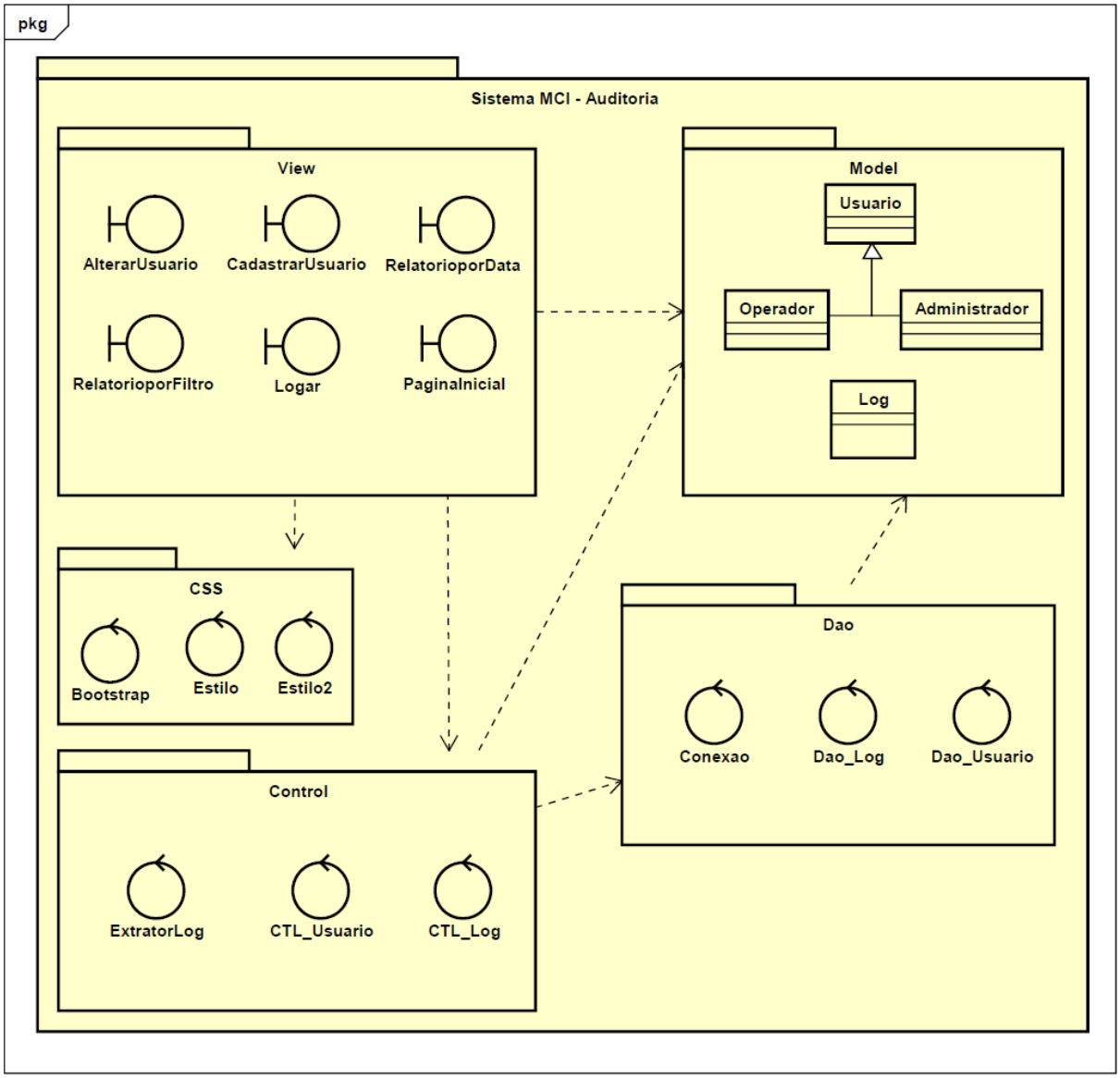


Figura 11 - Diagrama de Pacotes

Cada pacote teve uma finalidade no desenvolvimento do sistema, essas finalidades são descritas a seguir:

View: responsável pelo armazenamento das páginas, imagens, CSS entre outras partes, que faram interação com os usuários.

Model: responsável pelo armazenamento das classes dos objetos utilizados no sistema.

Control: responsável pelo armazenamento das regras de negócio, e as classes conexões com o banco de dados.

Dao: Esse pacote e responsável por toda interação com o banco de dados, como instruções de execução e SQL.

CSS: Esse pacote e responsável pelo armazenamento de todo código css utilizado para definir o estilo das páginas do sistema.

3.8 Diagrama Navegacional

A organização das telas de interação com os usuários foi organizada com nível de acesso, garantindo que usuários não autorizados acesse o sistema e que funcionalidades não sejam executadas por usuários não autorizados. A comunicação entre as telas está representada conforme Figura 12 - Diagrama de Máquina de Estados a seguir:

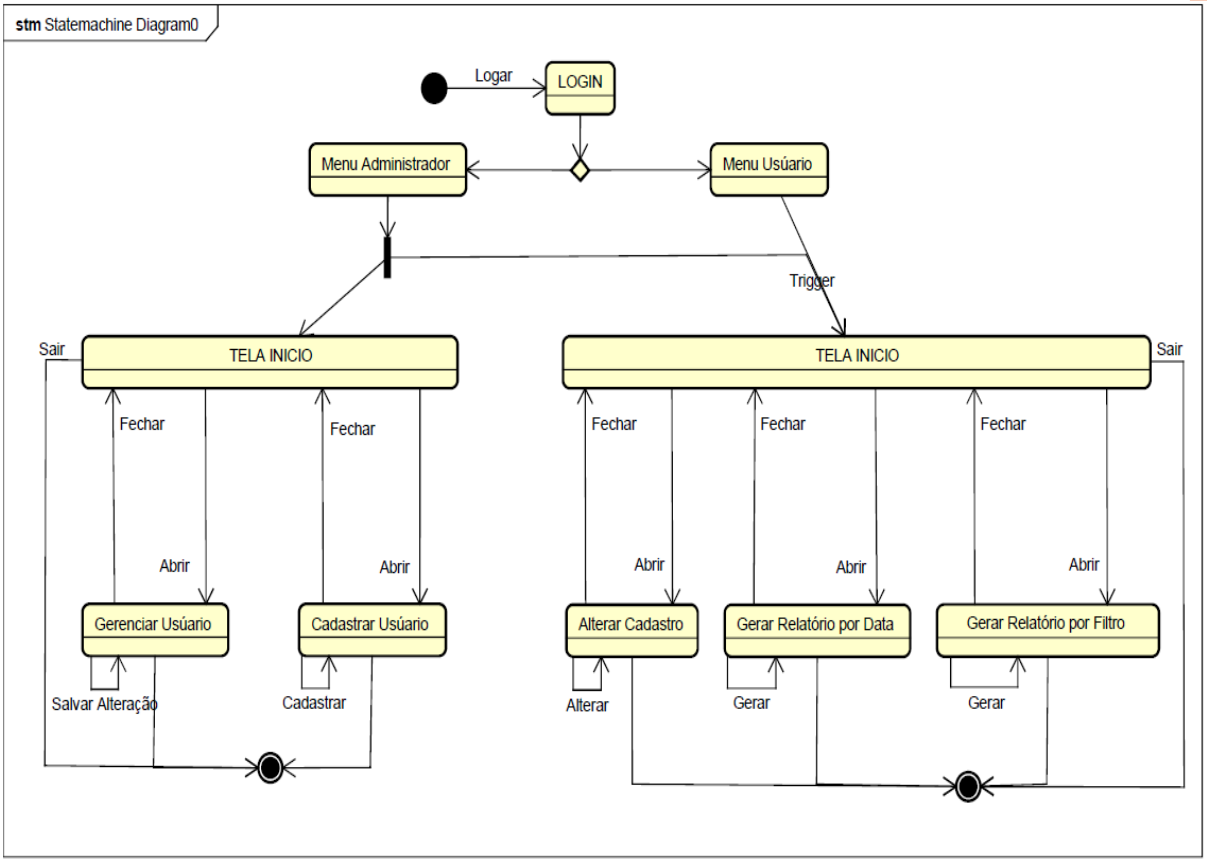


Figura 12 - Diagrama de Máquina de Estado

No Diagrama de Máquina de Estado pode-se identificar que para realizar o acesso ao sistema, somente será possível por meio de autenticação de usuário. Os usuários cadastrados no sistema após realizar a autenticação poderão acessar as funcionalidades ilustrada no diagrama conforme o seu nível de acesso.

Os usuários com nível de acesso Administrador terão acesso as funcionalidades do sistema e os usuários com nível de acesso Operador terão restrição ao acesso as funcionalidades de gerenciamento de usuário.

3.9 Diagrama de Sequência

Para executar as funcionalidades do sistema, é realiza a instância de classes e chamadas de métodos seguindo uma sequência. Cada classe e método no sistema é responsável pela execução de determinadas operações.

Para realizar o login no sistema o usuário fará a interação com a tela de login informando cpf e senha, após irá solicitar ao sistema que efetue o login, essa opção fará com que a tela instancie uma classe e seu respectivo método.

A instância das classes e chamadas dos métodos no processo de login mantem uma sequência, podendo ser observada essa sequência a seguir na Figura 13 - Diagrama de Sequência de Login:

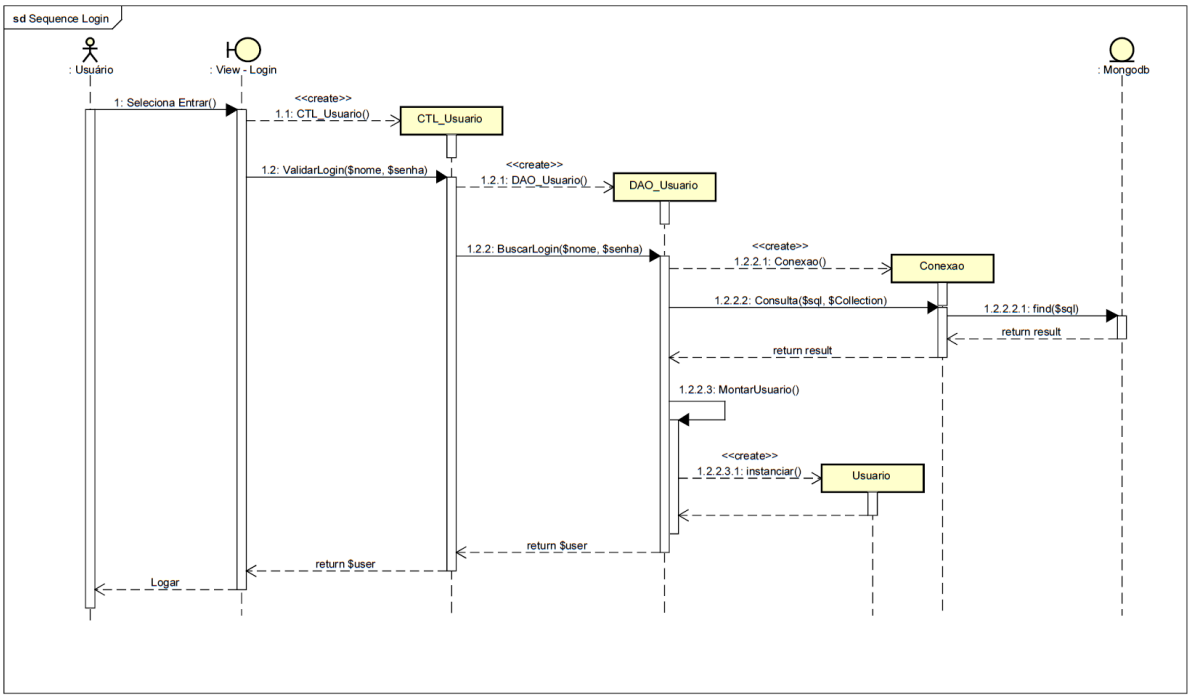


Figura 13 - Diagrama de Sequência de Login

O processo de extração de dados de log do Squid, segue a mesma lógica de sequência do processo de login na instância de classes e métodos, se diferenciando somente na interação do usuário com o sistema. O processo de extração não possui interação com o usuário, sendo executada por meio do Cron do Linux em um horário pré-determinado.

A instância das classes e chamadas dos métodos no processo de extração de dados do arquivo de log do Squid pode ser observada a seguir na Figura 14 - **Diagrama de Sequência Extração de Dados do Squid**:

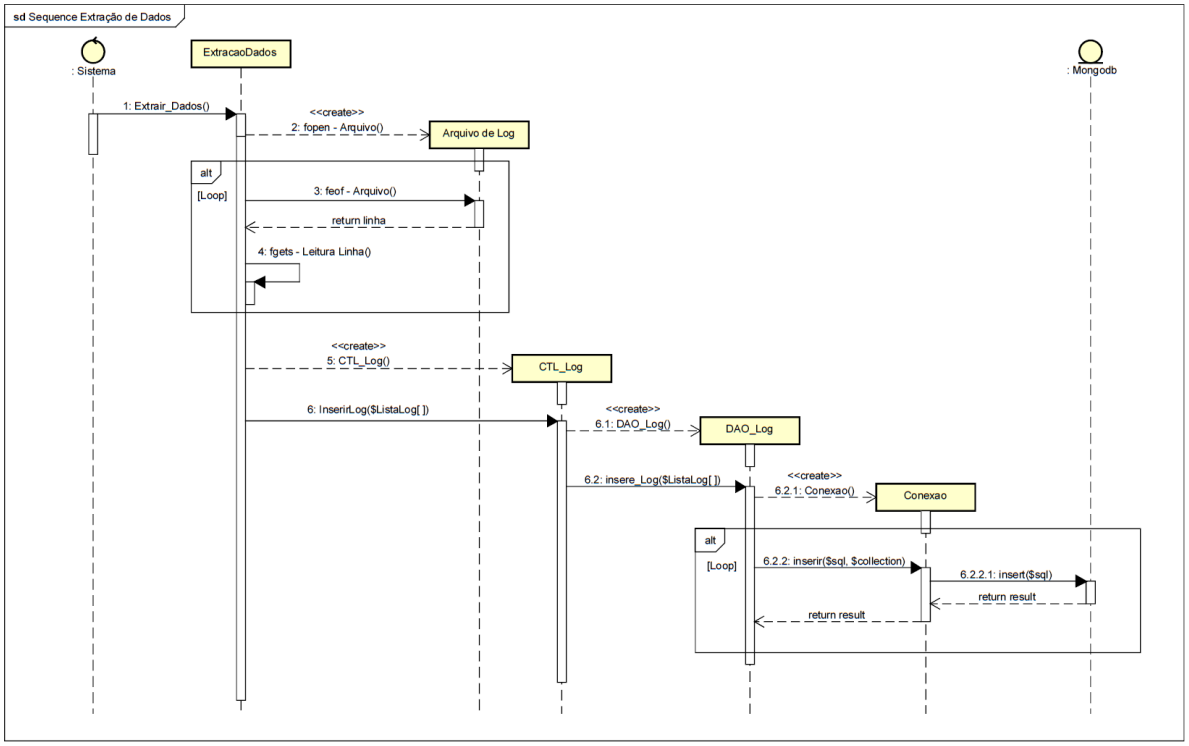


Figura 14 - Diagrama de Sequência Extração de Dados do Squid

O processo na geração dos relatórios segue o mesmo princípio da lógica do processo de login, somente diferenciando em um loop na chamada do método Montar_Log, que se refere aos log obtidos na consulta com o banco de dados.

A instância das classes e chamadas dos métodos no processo de gerar os relatórios pode ser observada a seguir na Figura 15 - **Diagrama de Sequência Relatório por Filtro**:

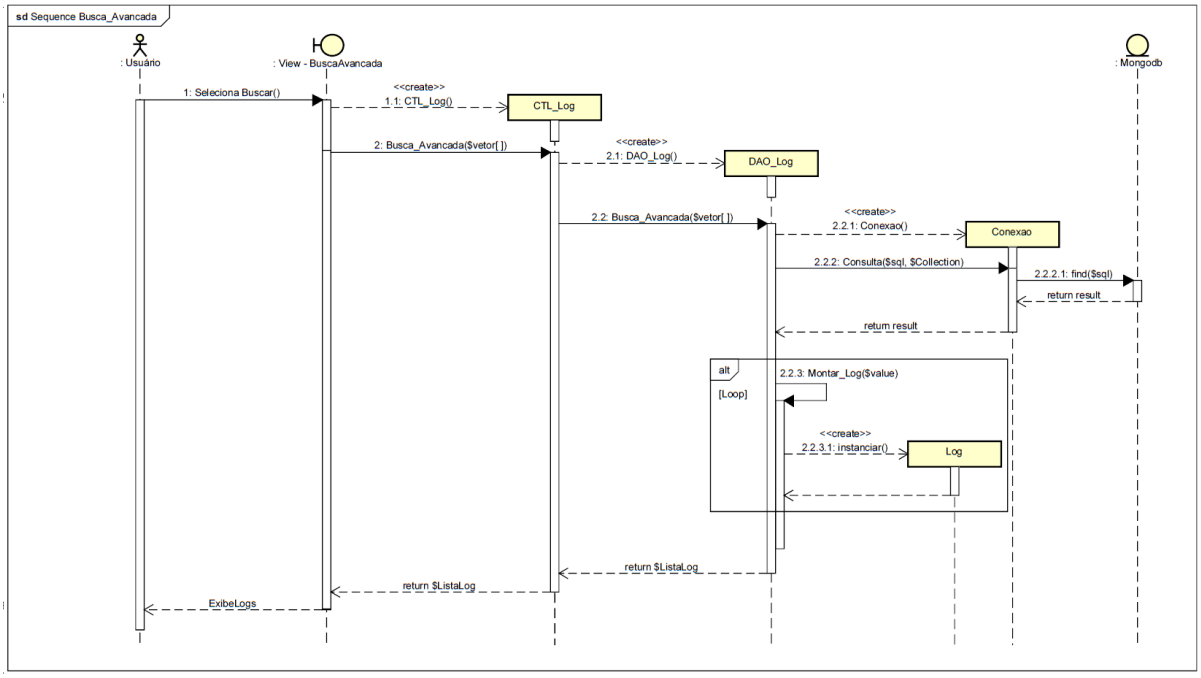


Figura 15 - Diagrama de Sequência Relatório por Filtro

3.10 Telas

As telas criadas nesse trabalho foram desenvolvidas pensando nas funcionalidades que o sistema possui. Cada tela possui especificações distintas visando as funcionalidades, e desenvolvidas para uma aplicação web.

Para acesso ao sistema foi desenvolvido uma tela para autenticação de usuário, tela de login. Para realizar o acesso o usuário após cadastrado no sistema deverá informar seu cpf e senha, caso os dados informados não condizerem com os dados cadastrados no sistema, a tela mostrará uma mensagem de erro para o usuário, desta forma impedindo seu acesso.

A tela de login desenvolvida para o sistema poderá ser visualizada a seguir na Figura 16 - **Tela de Login**:

Figura 16 - Tela de Login

No acesso dos usuários para com as funcionalidades do sistema foi desenvolvida uma tela de menu principal, A tela de menu principal contém atalhos para as funcionalidades do sistema, facilitando a localização dessas funcionalidades e seu acesso. A tela de menu principal pode ser observada a seguir na Figura 17 - Tela Página Principal:

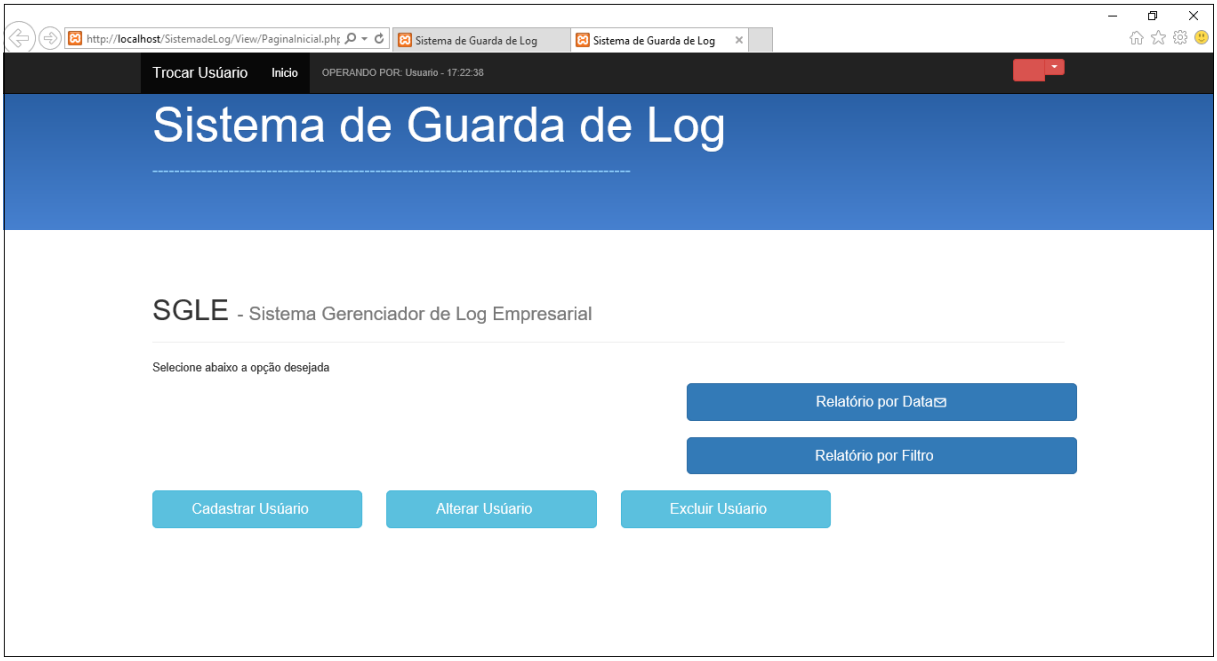


Figura 17 - Tela Página Principal

O sistema desenvolvido possibilita ao usuário realizar consultas baseadas em datas e intervalos de datas. Para essa funcionalidade foi desenvolvida uma tela, Tela de Relatório por Data, que permitirá ao usuário inserir datas nas consultas dos registros antes de gerar os relatórios. A Tela de Relatórios por Datas poderá ser vista a seguir na Figura 18 - Tela Relatório por Data:

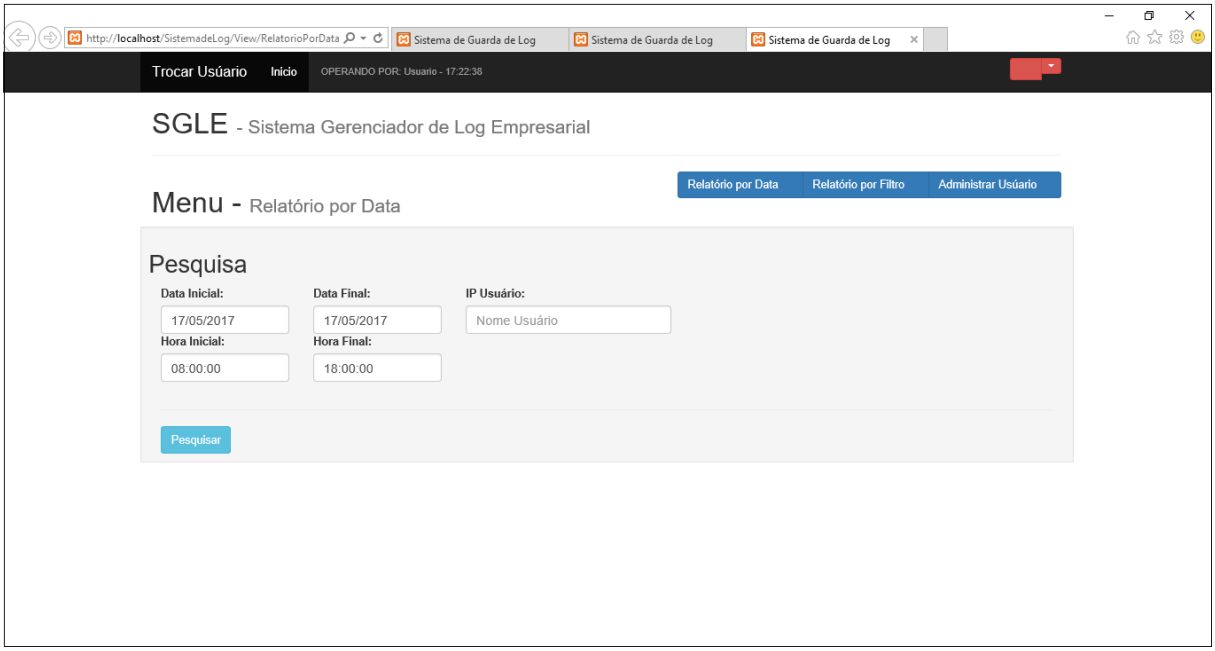


Figura 18 - Tela Relatório por Data

O sistema possibilita que o usuário realize consultas baseadas em filtros em suas consultas. Para gerar os relatórios por meio de filtros, foi desenvolvido uma tela para essa funcionalidade, a Tela Relatório por Filtro possibilita ao usuário a inserir parâmetros em consultas antes de gerar os relatórios. A Tela Relatórios por Filtro poderá ser visualizada a seguir na Figura 19 - Tela de Relatório por Filtro:

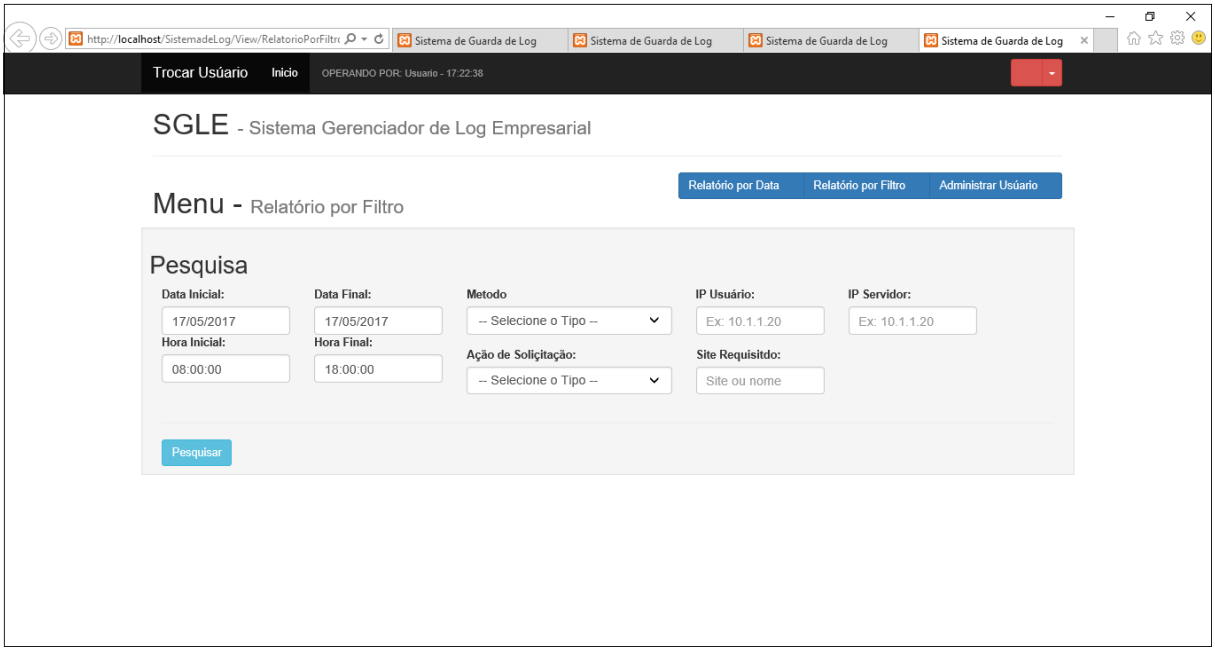


Figura 19 - Tela de Relatório por Filtro

3.11 Resultados

3.11.1 Comparativo de Ferramentas Similares

Nos dias de hoje pode-se encontrar na Internet uma grande variedade de ferramentas e software, livres ou proprietárias, para diversificados ramos ou funcionalidades distintas. Desta forma é possível encontrar na Internet várias ferramentas para com a mesma finalidade que o sistema desenvolvido nesse trabalho.

Cada sistema possui suas características e funcionalidades, podendo ser diferentes quando comparadas, e ainda podem realizar a mesma funcionalidade de formas diferentes, podendo até mesmo a funcionalidade não satisfazer as necessidades de seus usuários.

Analisando esses critérios foi realizado uma análise comparativa das ferramentas já desenvolvidas com o sistema desenvolvido nesse trabalho, com intuito de identificar o cumprimento de suas atividades, e verificar sua real necessidade de desenvolvimento. Para realizar esse comparativo foi analisado os cumprimentos dos sistemas para com as diretrizes impostas pela lei do Marco Civil da Internet.

A escolha das ferramentas para estudo e comparação se deu através de três características, sendo essas características utilizadas no sistema desenvolvido nesse trabalho, que são:

- Software licença livre;

- Desenvolvidas na plataforma web;
- Baseadas no Proxy Squid.

Com essas características as ferramentas escolhidas para serem comparadas entre as várias ferramentas disponíveis foi escolhido, então, o SARG, MYSAR e LIGHT SQUID como objetos de comparação.

Para identificar as características que cada sistema possui foi montada medidas que define os cumprimentos dos sistemas para com as exigências importas pela lei.

Desse modo, após a comparação das principais funcionalidades de cada ferramenta ser conceituada e analisada, cada uma delas recebeu uma medida de cumprimento para cada cumprimento de diretrizes. As medidas podem ser identificas a seguir na Tabela 17 **–** Cumprimento de Diretriz:

Tabela 17 – Cumprimento de Diretriz

Cumprimento	DEFINIÇÃO
	Atende ao Critério
	Atende Parcialmente ao Critério
	Não atende ao Critério

As diretrizes impostas pela lei que foram identificadas nesse trabalho serão classificadas por uma sequência, essa sequência irá iniciar de MC01 até MC06. Essa sequência facilitará a organização das diretrizes e a visualização dos resultados obtidos na comparação das ferramentas.

As diretrizes identificadas na lei do Marco Civil da Internet serão descritas e classificadas a seguir definidas em Presidência da República (2014):

MC01 – Segundo o Art. 7º da lei do Marco Civil da Internet (vide Anexo 01) refere-se ao exercício da cidadania, e assegura inviolabilidade e sigilo das comunicações pela Internet armazenados, salvo por ordem judicial.

O MC01 refere-se à capacidade do Sistema de manter os registros de conexão de seus usuários em um ambiente controlado. Para controlar o ambiente o sistema deve possuir autenticação de senha para acesso as funcionalidades do sistema.

MC02 - Segundo o Art. 10º da lei do Marco Civil da Internet (vide Anexo 01) refere-se sobre a disponibilização dos registros de conexão de Internet por meio da

ordem judicial. O responsável será obrigado a disponibilizar os registros, podendo associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal.

O MC02 refere-se à capacidade do sistema de identificar a origem do acesso. Para identificar a origem do acesso, o sistema deverá possibilitar a visualização de informações que identifique o terminal ou usuário (ou ambas) que realizou a requisição.

MC03 - Segundo o Art. 13º da lei do Marco Civil da Internet (vide Anexo 01) refere-se da provisão de conexão à Internet, cabendo ao administrador do sistema o dever de manter os registros de conexão, sob sigilo, pelo prazo de 1 (um) ano, e os registros de acesso a aplicações de Internet pelo prazo de 6 (seis) meses.

O MC03 refere-se à capacidade do sistema de armazenar o registro de conexão pelo prazo de 1 (um) ano e os registro de acesso a aplicações de Internet pelo prazo de 6 (seis) meses. Para realizar esse armazenamento, o sistema deverá possibilitar a gravação dos registros em um banco de dados, que se refere a um ambiente controlado e seguro.

MC04 - Segundo o Art. 18º da lei do Marco Civil da Internet (vide Anexo 01) refere-se ao provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes por terceiros. Deverá realizar a identificação clara e específica do conteúdo, que permita a localização inequívoca do material.

O MC04 refere-se à capacidade do sistema de identificar o real acesso que o usuário requisitou, de forma clara, permitindo a localização do material acessado. O sistema deverá permitir a administrador da rede o real acesso requisitado pelo usuário.

MC05 - Segundo o Art. 22º da lei do Marco Civil da Internet (vide Anexo 01) refere-se que a parte interessada poderá requerer em juízo o fornecimento de registros de conexão pelo período ao qual se referem os registros.

O MC05 refere-se à capacidade do sistema de gerar relatórios em períodos distintos e em intervalos de tempo. O sistema deverá possuir um filtro de busca nos registros permitindo selecionar datas ou intervalos de datas em suas consultas.

O MC06 é um complemento para o MC05 referente a usabilidade do sistema. O sistema deverá ser de fácil uso e entendimento, e possibilitar um rápido mecanismo de acesso aos registros de conexão armazenados.

Pode-se verificar a seguir, em resumo, os resultados dos comparativos das ferramentas, conforme sequência atribuída para com as diretrizes imposta pela lei do Marco Civil da Internet na Tabela 18 – Comparativos de Ferramentas:

Tabela 18 – Comparativos de Ferramentas

Características	Sarg	Light Squid	MySar	MCI-Auditoria
MC01	±	±	±	✓
MC02	✓	✓	✓	✓
MC03	✗	✗	✓	✓
MC04	✓	✓	✓	✓
MC05	✗	✗	✗	✓
MC06	±	±	±	✓

Os resultados obtidos nos comparativos ilustrados na Tabela 18 – Comparativos de Ferramentas pode-se ser verificado a seguir:

- MC01:

  - Sarg, Light Squid, MySar: Essas ferramentas atendem parcialmente ao critério devido, não possui nenhuma funcionalidade nativa de controle de acesso ao sistema, sendo possível somente por meio do sistema operacional.

  - MCI-Auditoria: Essa ferramenta possui um controle de acesso nativo para validação dos usuários através de nome de usuário e senha no acesso ao sistema.

- MC02:

  - Sarg, Light Squid, MySar e o MCI-Auditoria: Essas ferramentas atendem ao critério devido, listar informações necessárias para identificação do usuário e o terminal que realizou a requisição em seus relatórios. As informações contidas nos relatórios das 4 ferramentas possuem as mesmas informações e características, podendo ser observadas a seguir na Figura 20 - Relatório de Acesso do MySQL

Últimas Atividades do Usuário

IP ESTAÇÃO	USUÁRIO	HORA	BYTES	URL	STATUS
192.168.100.204	-	14:49:25	3905	http://rs564.rapidshare.com/img2/download_file.jpg	TCP_MISS/200
192.168.100.204	-	14:49:25	913	http://rs564.rapidshare.com/img2/pfeil_zu.jpg	TCP_MISS/200
192.168.100.151	-	14:49:20	71837	http://blstc.msn.com/br/gbl/css/6/GTL_SiteGeneric.css	TCP_MISS/200
192.168.100.151	-	14:49:19	3869	http://blstc.msn.com/br/gbl/css/6/02.css	TCP_MISS/200
192.168.100.151	-	14:49:19	1400	http://blstc.msn.com/br/intl/xpr/css/2/xpr_RatingArticle.css	TCP_MISS/200
192.168.100.151	-	14:49:19	4107	http://blstc.msn.com/br/intl/xpr/css/1/xpr_mostpopular.css	TCP_MISS/200
192.168.100.151	-	14:49:19	184	http://clsf.nspmotion.com/htm/MOVIE65608.HTM	TCP_MISS/304
192.168.100.151	-	14:49:19	10391	http://blstc.msn.com/br/intl/INTLChannels/css/13/ArticleAndPhotoGallery.css	TCP_MISS/200
192.168.100.151	-	14:49:19	2027	http://blstc.msn.com/br/chan/css/4/chan_pollservice.css	TCP_MISS/200
192.168.100.151	-	14:49:19	57741	http://blstc.msn.com/br/intl/INTLChannels/css/14/INTLChannel.css	TCP_MISS/200

Figura 20 - Relatório de Acesso do MySQL

- MC03:

  - Sarg e o Light Squid: Essas ferramentas não atendem ao critério mediante à não possuírem nenhuma interação com banco de dados, os dados contidos em seus relatórios originam-se diretamente do arquivo acess.log do Squid.

  - MySar e o MCI-Auditoria: Essas ferramentas atendem ao critério por meio de seus relatórios obterem os dados através de consultas em um banco dados.

- MC04:

  - Sarg, Light Squid, MySar e o MCI-Auditoria: Essas ferramentas atendem ao critério devido ser possível em seus relatórios visualizar e acessar o conteúdo real que o usuário requisitou. As visualizações das requisições dos usuários nas quatro ferramentas são similares, sendo exemplificada na Figura 21 - Relatório de Acesso MySQL:

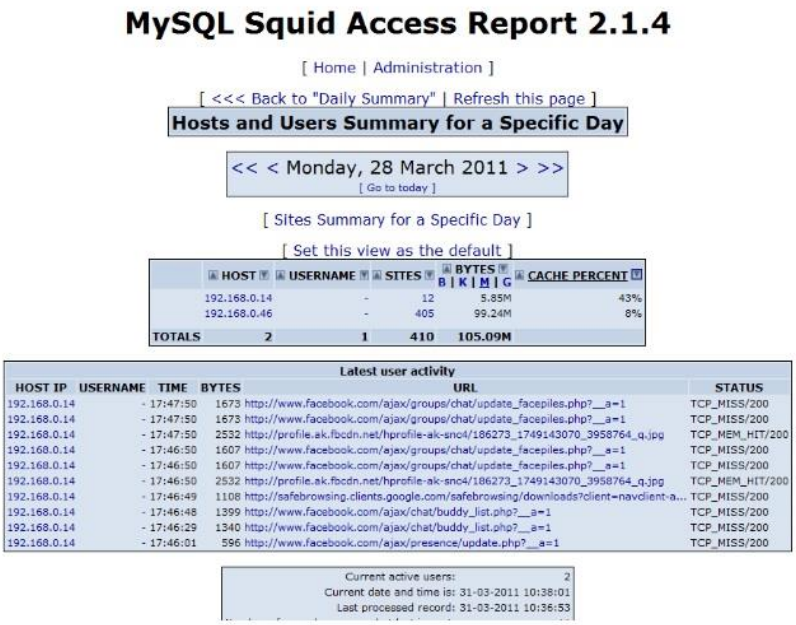


Figura 21 - Relatório de Acesso MySQL

- MC05:

  - Sarg, Light Squid e o MySar: Essas ferramentas não atendem ao critério mediante não possuírem filtros para consulta em períodos de tempo, seus relatórios são gerados somente por datas. As 3 ferramentas possuem as mesmas características de filtro de consultas, sendo exemplificada a segui na Figura 22 - Filtros de Consulta Ligh Squid:

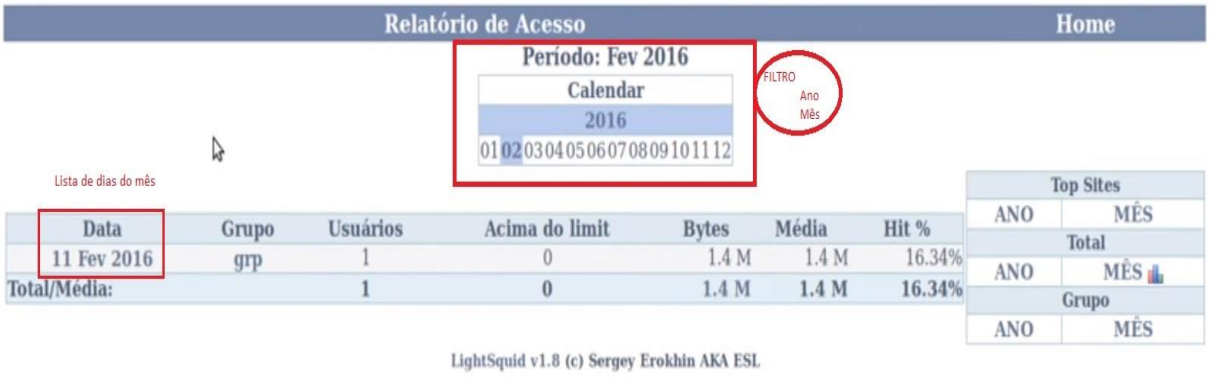


Figura 22 - Filtros de Consulta Ligh Squid

- MCI-Auditoria: Essa ferramenta atende ao critério, uma vez que suas consultas na emissão de seus relatórios serem dinâmicos, gerando relatórios mediante a necessidade do usuário, como, selecionar intervalos de tempos nas consultas para gerar os relatórios. Os filtros

dos relatórios do MCI-Auditoria podem ser observados a seguir na Figura 23 - Filtro de Relatório MCI-Auditoria:

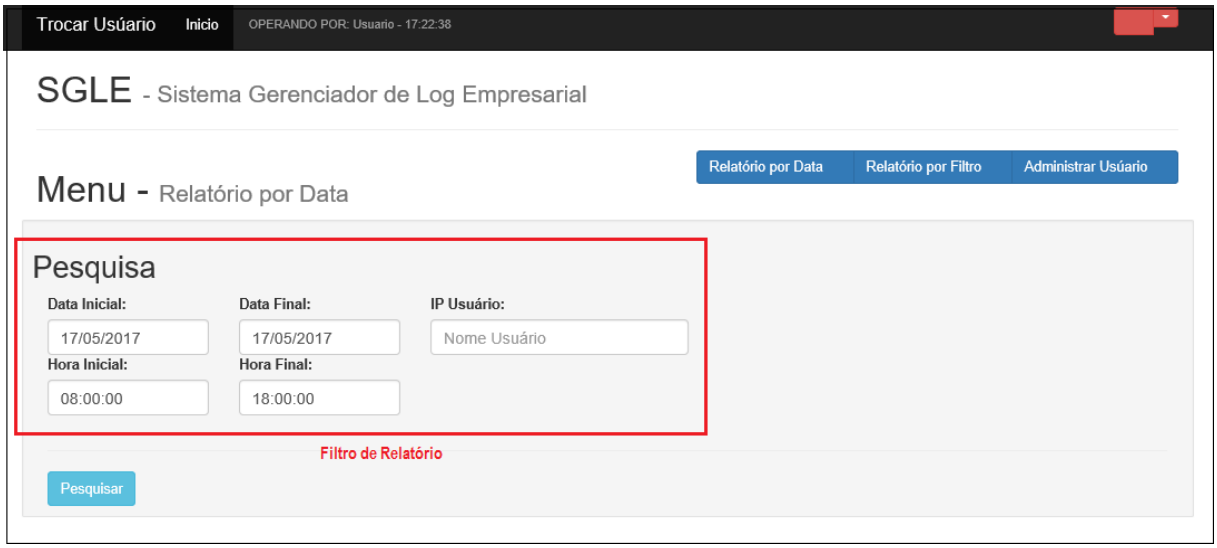


Figura 23 - Filtro de Relatório MCI-Auditoria

- MC06:

  - Sarg, Light Squid e o MySar: Essas ferramentas atendem parcialmente ao critério devido possuírem um fácil entendimento das funcionalidades, mais seus relatórios são baseados somente em data, tendo que o usuário selecionar ano, após mês e após dia e até usuário para localizar os registros desejados, tornando a localização do registro demorada e custosa.

  - MCI-Auditoria: Essa ferramenta atende ao critério porque em sua página inicial é possível o acesso a qualquer funcionalidade do sistema, tornando fácil a localizar e a usabilidade e em seus relatórios, com a opções de seleção de filtros o acesso aos registros se tornam rápidos e precisos mediante as necessidades do usuário.

3.11.2 Simulação de Teste do Sistema

Com intuito de validar as funcionalidades do sistema desenvolvido nesse trabalhado, foi criado simulações de possíveis cenários que possam ocorrer. Esses cenários foram elaborados pensando nas ocorrências que uma ordem judicial possa a vim solicitar para com a empresa.

Para desenvolvimento desses cenários foi definido três possíveis ocorrências. Os cenários e as soluções dos cenários desenvolvidos para validação do sistema, podem-se ser constados a seguir:

- V01 – Foi constado que o IP da empresa, está realizando postagens de conteúdo impróprios e ofensivos na data xx/xx/xxxx entre os horário xx:xx:xx e xx:xx:xx.

Para identificar o usuário (ou usuários) que realizou (realizaram) o acesso para a classificação V01, gerou-se no sistema um relatório em Relatórios por Data. O relatório foi baseado em realizando à busca nos registros armazenados no banco em uma data específica aplicando um intervalo de horários, que pode sem observado a seguir na Figura 24 - Filtro Relatório V01:

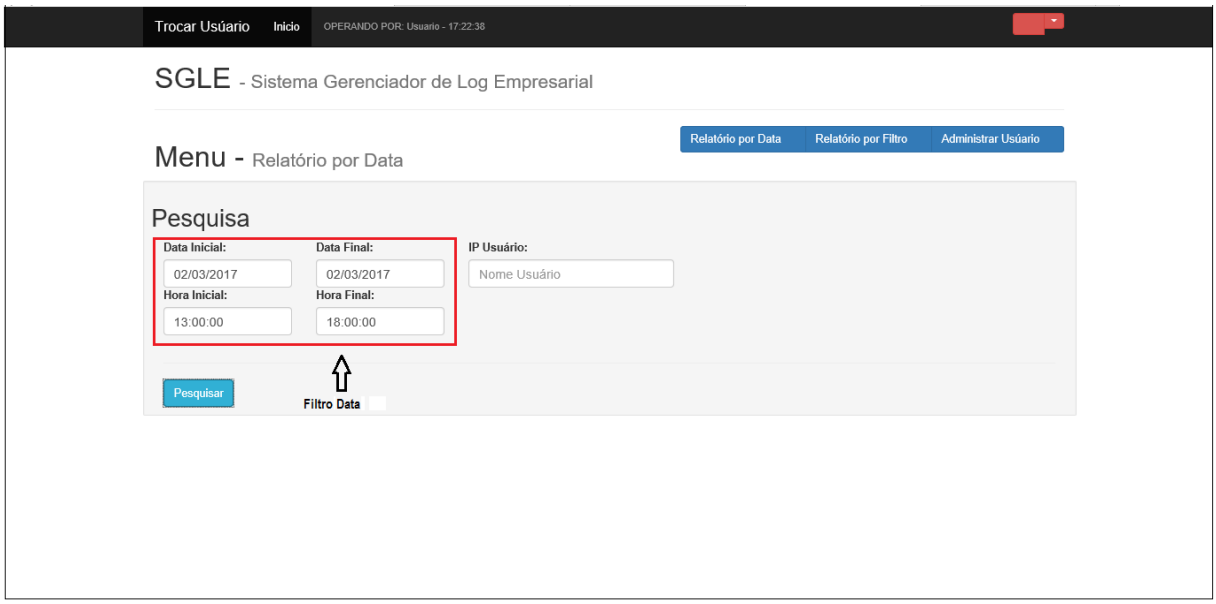


Figura 24 - Filtro Relatório V01

O resultado desse relatório contempla as informações necessárias para identificar os acessos realizados pelos usuários, em uma data específica com intervalo de hora. O relatório possui informações como, data e hora do acesso, usuário que realizou a solicitação, o IP do computador utilizado para acesso, o endereço acessado e o IP do servidor requisitado. O resultado do relatório pode ser visto a seguir na Figura 25 - Relatório V01:

Pesquisar

Data Acesso	Hora Acesso	Usuário	IP Requisitante	Endereço Acessado	IP Servidor
02/03/2017	16:32:18	HenriqueCONT	10.1.1.10	http://ocsp.godaddy.com/	188.121.36.239
02/03/2017	16:37:18	HenriqueCONT	10.1.1.10	http://ocsp.godaddy.com/	188.121.36.239
02/03/2017	16:42:19	HenriqueCONT	10.1.1.10	http://ocsp.godaddy.com/	188.121.36.239
02/03/2017	16:48:13	HenriqueCONT	10.1.1.10	http://www.google.hu/search?	74.125.232.216
02/03/2017	16:53:13	HenriqueCONT	10.1.1.10	http://www.google.hu/csi?	74.125.232.216
02/03/2017	16:58:16	HenriqueCONT	10.1.1.10	http://www.google.hu/url?	74.125.232.216
02/03/2017	17:03:16	HenriqueCONT	10.1.1.10	http://szabilinux.hu/squid3/index.html	87.229.23.46
02/03/2017	17:10:54	JoaoRH	10.1.1.20	http://173.193.216.165/iavs5x/servers.def.vpx	173.193.216.165
02/03/2017	17:15:55	JoaoRH	10.1.1.20	http://download722.avast.com/iavs5x/prod-ais.vpx	74.86.245.123
02/03/2017	17:20:57	JoaoRH	10.1.1.20	http://www.msftncsi.com/ncsi.txt	213.199.181.90
02/03/2017	17:26:00	JoaoRH	10.1.1.20	http://download965.avast.com/iavs5x/servers.def.vpx	74.86.245.116
02/03/2017	17:31:00	JoaoRH	10.1.1.20	http://download339.avast.com/iavs5x/prod-ais.vpx	109.123.114.42
02/03/2017	17:36:01	JoaoRH	10.1.1.20	http://download339.avast.com/iavs5x/part-jrog2-3e5.vpx	109.123.114.42
02/03/2017	17:41:01	JoaoRH	10.1.1.20	http://download339.avast.com/iavs5x/jrog2-3e3-3e2.vpx	109.123.114.42
02/03/2017	17:46:01	JoaoRH	10.1.1.20	http://download339.avast.com/iavs5x/jrog2-3e4-3e3.vpx	109.123.114.42
02/03/2017	17:51:01	JoaoRH	10.1.1.20	http://download339.avast.com/iavs5x/jrog2-3e5-3e4.vpx	109.123.114.42
02/03/2017	17:56:09	HenriqueCONT	10.1.1.10	http://www.google.hu/complete/search?	74.125.232.216

Figura 25 - Relatório V01

- V02 – Realizou-se um acesso não permitido do IP da empresa para com o site X na data entre xx/xx/xxxx e xx/xx/xxxx.

Para identificar o usuário (ou usuários) que realizou o acesso para a classificação V02, gerou-se no sistema um relatório em Relatórios por Filtro. O relatório buscou-se em realizar à busca nos registros armazenados no banco em um intervalo de data, utilizando o campo de filtro “Site” na consulta, que pode ser observado a seguir na Figura 26 - Filtro Relatório V02:

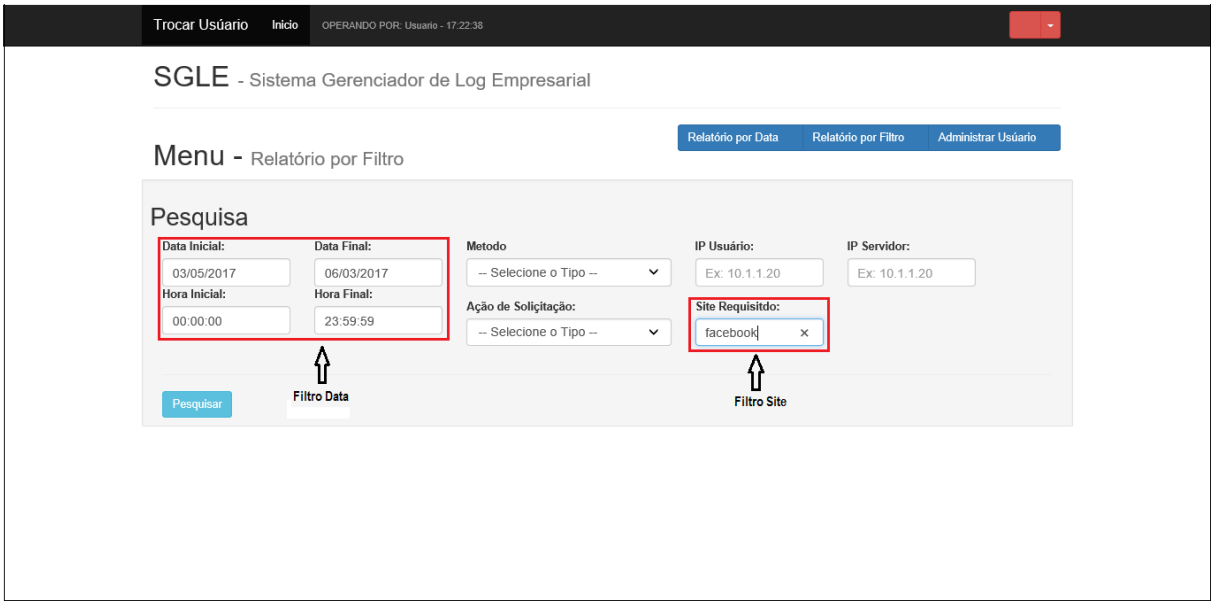
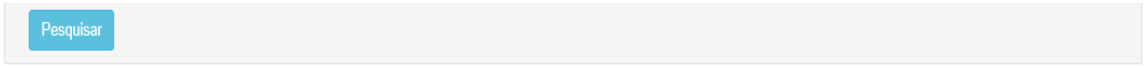


Figura 26 - Filtro Relatório V02

O resultado desse relatório contempla as informações necessárias para identificar os acessos realizados pelos usuários, em um intervalo de data em um site

específico. O relatório possui informações como, data e hora do acesso, usuário que realizou a solicitação, o IP do computador utilizado para acesso, o endereço acessado e o IP do servidor requisitado. O resultado do relatório pode ser visto a seguir na Figura 27 - Relatório V02:



Data Acesso	Hora Acesso	Usuário	Ação Tomada	IP Usúario	IP Servidor	Endereço Acessado	Metodo	Requisição
03/03/2017	11:50:21	HenriqueCONT	TCP_MISS/304	10.1.1.10	2.21.111.139	http://connect.facebook.net/en_US/all.js	GET	HIER_DIRECT
03/03/2017	14:05:23	HenriqueCONT	TCP_MISS/200	10.1.1.10	69.171.242.13	http://www.facebook.com/plugins/like.php?	GET	HIER_DIRECT
03/03/2017	14:10:23	HenriqueCONT	TCP_MISS/200	10.1.1.10	69.171.242.13	http://www.facebook.com/plugins/like.php?	GET	HIER_DIRECT
03/03/2017	18:59:26	HenriqueCONT	TCP_REFRESH_UNMODIFIED/304	10.1.1.10	195.228.252.138	http://hup.hu/images/powered/facebook.png	GET	HIER_DIRECT
03/03/2017	23:04:28	HenriqueCONT	TCP_MISS/200	10.1.1.10	69.171.242.14	http://www.facebook.com/plugins/like.php?	GET	HIER_DIRECT
04/03/2017	01:24:29	HenriqueCONT	TCP_MISS/200	10.1.1.10	69.171.242.14	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
04/03/2017	04:05:07	JoaoRH	TCP_MISS/200	10.1.1.20	2.21.111.139	http://connect.facebook.net/hu_HU/all.js	GET	HIER_DIRECT
04/03/2017	06:05:13	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
04/03/2017	10:35:18	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/like.php?	GET	HIER_DIRECT
04/03/2017	11:00:18	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/like.php?	GET	HIER_DIRECT
04/03/2017	11:05:18	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/like.php?	GET	HIER_DIRECT
05/03/2017	00:56:06	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
05/03/2017	01:51:21	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
05/03/2017	03:58:20	JoaoRH	TCP_MISS/304	10.1.1.20	2.21.111.139	http://connect.facebook.net/hu_HU/all.js	GET	HIER_DIRECT
05/03/2017	04:08:21	JoaoRH	TCP_MISS/200	10.1.1.20	66.220.156.32	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
05/03/2017	04:38:31	JoaoRH	TCP_MISS/200	10.1.1.20	66.220.156.32	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
05/03/2017	08:36:51	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
05/03/2017	08:56:57	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
05/03/2017	09:58:11	JoaoRH	TCP_MISS/304	10.1.1.20	2.21.111.139	http://connect.facebook.net/hu_HU/all.js	GET	HIER_DIRECT
05/03/2017	10:13:13	JoaoRH	TCP_MISS/200	10.1.1.20	69.171.242.14	http://www.facebook.com/plugins/likebox.php?	GET	HIER_DIRECT
06/03/2017	23:10:21	HenriqueCONT	TCP_MISS/304	10.1.1.10	2.21.111.139	http://connect.facebook.net/en_US/all.js	GET	HIER_DIRECT

Figura 27 - Relatório V02

- V03 – Constou-se uma ocorrência de acesso do IP da empresa para com o site X, o acesso ocorreu na data xx/xx/xxxx no horário xx:xx:xx. É solicitado que identifique o usuário que originou o acesso.

Para identificar o usuário que realizou o acesso para a classificação V03, gerou-se no sistema um relatório em Relatórios por Filtro. O relatório buscou-se em realizando à busca nos registros armazenados no banco em uma data e horário especifico, utilizando o filtro “Site”, que pode sem observado a seguir na Figura 28 - Filtro Relatório V03:

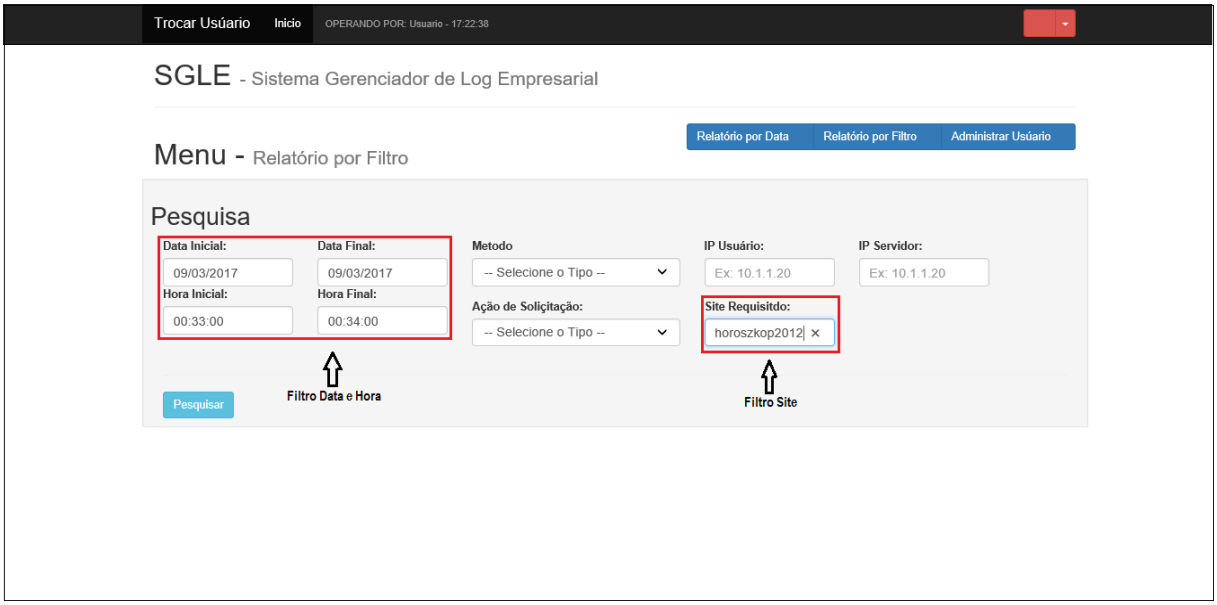


Figura 28 - Filtro Relatório V03

O resultado desse relatório contempla as informações necessárias para identificar o acesso realizado pelo usuário, em uma data, horário e site especifico. O relatório possui informações como, data e hora do acesso, usuário que realizou a solicitação, o IP do computador utilizado para acesso, o endereço acessado e o IP do servidor requisitado. O resultado do relatório pode ser visto a seguir na Figura 29 - Relatório V03:

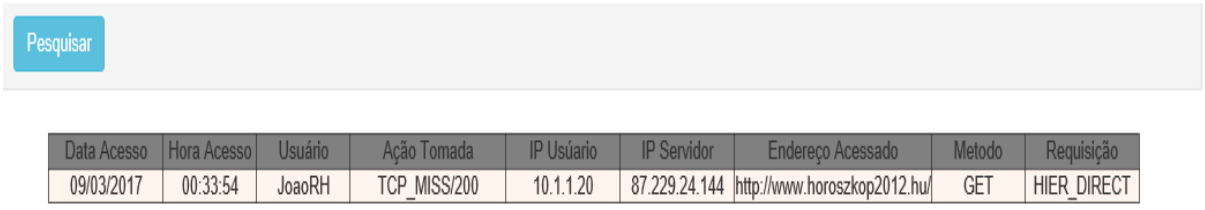


Figura 29 - Relatório V03

O sistema possibilitou realizar buscas em intervalos de tempo e identificar o usuário que realizou o acesso, assim cumprindo para com as solicitações realizadas através dos três cenários criados para validação da ferramenta.

Pode-se desta forma concluir a validação do sistema com êxito para com seu propósito. Com a possibilidade de realizar buscas utilizando filtros nos registros armazenado em banco, facilita a identificação do usuário ou acesso, desta forma satisfazendo as diretrizes imposta pela lei do Marco Civil da Internet.

4. CONCLUSÕES

Este trabalho apresentou uma abordagem que identifica os impactos e as dificuldades das organizações com as exigências imposta no surgimento da Lei o Marco Civil da Internet, em seu pilar de Privacidade.

A abordagem apontou que provedores de Internet devem realizar o armazenamento dos registros de conexões de seus usuários em um ambiente controlado salvo somente por ordem judicial. Quando essas organizações forem notificadas judicialmente, cria-se a necessidade de identificar a origem do acesso alvo de investigação, quando possuir mais de um usuário conectado à Internet.

Com esse cenário foi feito uma análise nas ferramentas disponíveis, que pode ser constado que não atenderam à todas as diretrizes que a lei impôs, em referência ao tempo de armazenamento dos registros e na identificação da origem do acesso à o conteúdo na Internet.

O desenvolvimento de uma ferramenta se fez necessário para satisfazer essas diretrizes que a lei impôs, tendo como princípio à identificação do ponto que originou o acesso ou conteúdo e nos prazos de armazenamento dos registros.

A ferramenta desenvolvida nesse trabalho, permite que seja realizado o armazenamento dos registros de conexão em um banco de dados. Com esses registros armazenados em banco, e a ferramenta possibilitar relatórios baseados em filtros se torna possível a análise desses registros. Neste contexto, a ferramenta possibilita a identificação quando necessário, do ponto que realizou o acesso ou conteúdo na Internet.

A ferramenta desenvolvida nesse trabalho, foi comparada e validada suas funcionalidades, possibilitando a validação da ferramenta em seu cumprimento para com as diretrizes impostas na lei nº 12.965/2014 – Marco Civil da Internet.

Como trabalhos futuros podem ser enumerados os seguintes temas:

1 – Com os registros armazenados em um banco de dados, possibilita à aplicação de uma ferramenta ou criação de um módulo no sistema, que possibilite gerar relatórios baseados em mineração de dados. Aplicando mineração de dados nos registros armazenados pode-se extrair informações úteis para o usuário do sistema, por exemplo, identificar a quantidade de tempo gasto dos usuários em sites

não relacionadas ao trabalho, quantidade de banda utilizada pelo os usuários, horários de pico de consumo de banda entre outros.

2 – A aplicação de ferramentas de teste da Engenharia de Software como Apodora (ferramenta de avaliação de interface), Apache Jmater (ferramenta de avaliação de performance), Redmine (ferramenta para localizar bugs no desenvolvimento) entre outros, pode garantir melhor desempenho do sistema e uma melhor interação para com o usuário.

3 – O módulo de extração de dados do sistema será executado por meio do Cron do sistema Operacional, realizando a extração dos logs do arquivo Access.log do Squid. Essa execução por meio do Cron pode inviabilizar o sistema desenvolvido se não for tratado corretamente. Mediante a esse fato, se faz necessário o estudo e levantamento dos requisitos dessa funcionalidade mediante sua complexidade para implantação.

O sistema desenvolvido nesse trabalho é um projeto Open Source, seu código fonte está disponível no endereço eletrônico https://github.com/Ederson-Vilela/Sistema-para-relat-rio-de-Log-do-Squid.

REFERÊNCIAS

CGI.BR (Org.). **O CGI.br e o Marco Civil da Internet:** Defesa da privacidade de todos que utilizam a Internet; Neutralidade de rede; Inimputabilidade da rede. 2013. Disponível em: <http://www.cgi.br/publicacao/o-cgi-br-e-o-marco-civil-da-internet/>. Acesso em: 07 set. 2016.

CONCEIÇÃO, Matheus Weber da. OCTOPUS: FERRAMENTA DE CÓDIGO ABERTO PARA GERAÇÃO DE RELATÓRIOS PARA O SERVIDOR PROXY SQUID. 2012. 82 f. TCC (Graduação) - Curso de CiÊncia da ComputaÇÃo, Universidade do Vale do Itajai, Itajai, 2012.

COSA, Eduardo Augusto. **Controle de acesso através do Squid**. Bazar: Software e Conhecimento Livres**,** Lavras (mg), v. 1, n. 1, p.67-78, jul. 2006.

DIAS, Tatiana de Mello. **Chile aprova lei de neutralidade na rede.** 2010. Disponível em: <http://link.estadao.com.br/noticias/geral,chile-aprova-lei-de-neutralidade-na-rede,10000042918>. Acesso em: 27 out. 2016.

BRASIL, Governo Federal do, CULTURA, Ministério da. **Regulamentação da Internet na Itália – Contribuição do Itamaraty.** 2010. Disponível em: <http://culturadigital.br/marcocivil/2010/06/10/regulamentacao-da-internet-na-italia-contribuicao-do-itamaraty/>. Acesso em: 04 dez. 2016.

——— **Regulamentação da Internet na Espanha – Contribuição do Itamaraty.** 2010. Disponível em: <http://culturadigital.br/marcocivil/2010/06/09/regulamentacao-da-internet-na-espanha-contribuicao-do-itamaraty>. Acesso em: 04 dez. 2016.

História da Internet. 2016. Disponível em: <https://www.todamateria.com.br/historia-da-internet/>. Acesso em: 04 dez. 2016.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet:** Uma abordagem top-down. 3 ed. São Paulo: Pearson Addison Wesley, 2006.

LUNARDI, Marco **Agisander - Squid: Prático e didático** - 1ª Ed., Editora Ciência Moderna, 2005.

MACÊDO, Diego. Proxy Cache e Reverso. 2016. Disponível em: <http://www.diegomacedo.com.br/proxy-cache-e-reverso/?print=pdf>. Acesso em: 18 dez. 2016.

MCCABE, James D. **Network Analysis, Architecture, and Design.** 3 ed. Burlington: Morgan Kaufmann Publishers, 2007.

NETO, Urubatan: **Dominando Linux Firewall Iptables:** Linguagem de Programação. 1ª edição. Rio de Janeiro: Ciência Moderna Ltda, 2004. 98 p.

ORSO, P. SARG: **Squid Analysis Report Generator**. [S.l.], [2006?]. Disponível em: <http://sarg.sourceforge.net>. Acesso em: 29 mar. 2006.

PRESIDÊNCIA DA REPÚBLICA. Congresso. Senado. Constituição (2014). Lei nº 12.965, de 23 de abril de 2014. Estabelece Princípios, Garantias, Direitos e Deveres Para O Uso da Internet no Brasil.: Marco Civil da Internet. Brasília, DISTRITO FEDERAL, 23 abr. 2014.

PONTES, Elvis; HIRATA, Sérgio; HONÓRIO, Solli. **Segurança e Aceleração de Internet:** Utilização de Proxy Servers para manutenção de WEB. Disponível em: <http://www.pontes.inf.br/docs/proxy.pdf>. Acesso em: 07 set. 2016.

RICCI, Bruno; MENDONÇA, Nelson - **Squid: Solução Definitiva** - 1ª Ed., Editora Ciência Moderna, 2006.

TUTORIALS POINT. Proxy Server. 2016. Disponível em: <https://www.tutorialspoint.com/internet_technologies/proxy_servers.htm>. Acesso em: 18 dez. 2016.

WESSELS, Duane. **Squid: The Definitive Guide. Sebastopol**: O Reilly, 2004.

ANEXO 01

Presidência da República
Casa Civil
Subchefia para Assuntos Jurídicos

LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II
Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5ºda Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV
Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no **caput**, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF

José Eduardo Cardozo

Miriam Belchior

Paulo Bernardo Silva

Clélio Campolina Diniz