UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS APLICADAS A EDUCAÇÃO

DEPARTAMENTO DE CIÊNCIAS EXATAS

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

Sigilo e Ambiente Controlado baseado no Marco Civil da Internet e na NBR 27002

AUTOR Diego Nascimento da Silva

Orientador: Prof. Dr. Carlos Eduardo Silveira Dias

RIO TINTO - PB

Março/2015

AUTOR Diego Nascimento da Silva

Sigilo e Ambiente Controlado Baseado no Marco Civil da Internet e na NBR 27002

Monografia apresentada para obtenção do título de Bacharel à banca examinadora no Curso de Bacharelado em Sistemas de Informação do Centro de Ciências Aplicadas e Educação (CCAE), Campus IV da Universidade Federal da Paraíba.
Orientador: Prof. Dr. Carlos Eduardo Silveira Dias.

RIO TINTO – PB
Março/2015

S586s Silva, Diego Nascimento da.

1.1.1.1 Sigilo e ambiente controlado baseado no Marco Civil da Internet e na NBR 27002. / Diego Nascimento da Silva. – Rio Tinto: [s.n.], 2015.

46 f. : il. –

Orientador: Prof. Dr. Carlos Eduardo Silveira Dias.
Monografia (Graduação) – UFPB/CCAE.

1. Segurança da informação. 2. Internet - marco civil. 3. NBR 27002.

UFPB/BS-CCAE
CDU: 004:658(043.2)

Diego Nascimento da Silva

Sigilo e Ambiente Controlado baseado no Marco Civil da Internet e na NBR 27002

Trabalho de Conclusão de Curso submetido ao Curso de Bacharelado em Sistemas de Informação da Universidade Federal da Paraíba, Campus IV, como parte dos requisitos necessários para obtenção do grau de BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Assinatura do autor:_____

APROVADO POR:

_____
Orientador: Prof. Dr. Carlos Eduardo Silveira Dias
Universidade Federal da Paraíba – Campus IV

_____
Prof. Me. Rafael Marrocos Magalhães
Universidade Federal da Paraíba – Campus IV

_____
Prof. Dr. Alexandre Scaico
Universidade Federal da Paraíba – Campus IV

RIO TINTO - PB
Março/2015

"Se eu vi mais longe, foi por estar de pé sobre ombros de gigantes." Isaac Newton

AGRADECIMENTOS

A Deus por seu eterno amor e por estar sempre presente em cada momento da minha vida e a Maria Santíssima por sempre interceder por mim.

A minha Mãe por seu exemplo de mãe, mulher e filha. Uma verdadeira guerreira, que sempre fez de tudo por mim.

A minha família de sangue e a de coração (Família Amorim), por ser meu porto seguro, por estar comigo nos momentos mais felizes e nos mais tristes que vivi. Por acreditarem em mim, sempre me incentivando nos estudos.

A minha namorada Mayara, por seu companheirismo e por sempre acreditar e confiar na minha vida acadêmica e profissional.

Aos meus SEMPRE AMIGOS, pela confiança, motivação e exemplos na vida e nos estudos. Com eles sei que posso confiar sempre.

Aos colegas de Curso que seguiram juntos comigo nessa difícil caminhada, me apoiando sempre que precisei, me incentivando a não desistir. Estes em especial quero sempre presente em minha vida (Giordania, Simone, Paulo Antonio, Vicente Neto, Francisco Ihago).

A todos os professores que transmitiram seus conhecimentos ao longo da minha vida, minha eterna gratidão. E em especial a minha eterna diretora (Tia Belca), pois com ela vivi os meus melhores anos escolares, aprendendo como ser uma pessoa de bem através de seus ensinamentos e do seu caráter.

Aos professores do Curso de Sistemas de Informação e em especial ao meu orientador Carlos Dias (Hacks) por sua paciência, pela confiança depositada em mim e no meu trabalho e me incentivando a ir sempre mais além.

RESUMO

O Marco Civil é uma Lei para estabelecer os direitos, deveres e responsabilidades no uso da Internet no Brasil, sustentando princípios como a neutralidade da rede, privacidade e liberdade de expressão As organizações – empresas e instituições – que fornecem Internet agora são consideradas como provedores de acesso e tiveram suas responsabilidades aumentadas, sendo necessário armazenar de forma sigilosa e segura os registro de conexão dos seus usuários para futuras investigações, caso necessário. Como uma instituição, a UFPB fornece meios de acesso a Internet para toda a comunidade acadêmica e como tal deve se adequar ao Marco Civil da Internet.

Assim este trabalho propõe utilizar os Laboratórios de Informática do Campus IV da UFPB considerando este ambiente para uma proposta de analisar e validar os aspectos de registro de conexão sob sigilo e ambiente controlado do Marco Civil da Internet. Após análise detalhada dos aspectos sobre registro de conexão, sigilo e ambiente controlado, a NBR 27002 foi utilizada como guia de implementação de um sistema de gerenciamento para registro de atividades dos Laboratórios de Informática do Campus IV, realizando uma proposta inicial de adequação do Marco Civil da Internet através do uso da NBR 27002. E através destes estudos lançaremos uma proposta inicial para o gerenciamento dos registros de conexão dos estudantes em ambientes controlados e de maneira sigilosa.

Palavras chave: Segurança da Informação, Marco Civil da Internet, NBR, Sigilo, Ambiente Controlado, Análise, Registro de Conexão.

ABSTRACT

The Marco Civil is a law to establish the rights, duties and responsibilities in the use of Internet in Brazil, supporting principles such as net neutrality, privacy and freedom of expression. Organizations - companies and institutions - that provide Internet are now considered as service providers and had their increased responsibilities, requiring store confidentially and securely connection log of its users for further investigations if necessary . The UFPB is an institution that provides means of Internet access for the entire academic community and as such should suit the Marco Civil.

So this paper proposes to use the Computer Labs of Campus IV UFPB considering this setting for a proposal to review and validate aspects of connection log, confidential and controlled environment the Marco Civil of Internet. After detailed analysis of aspects of connection log, confidential and controlled environment, the NBR 27002 was used as a guide for introducing a management system for the Campus Computer Labs IV activity log, performing an initial proposal to adapt the Marco Civil Internet through the use of ISO 27002. And through these studies will launch an initial proposal for the management of students of the connection logs in controlled environments and confidentially.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

NBR – Norma Brasileira

SUMÁRIO

1 INTRODUÇÃO

Nas últimas décadas vivemos uma verdadeira revolução digital onde a cada ano mais pessoas tem acesso a novas tecnologias como computadores, *tablets* e *smartphones*. Aliado ao desenvolvimento e evolução destas tecnologias está à comunicação em rede, mas precisamente a rede mundial de computadores – Internet. Em decorrência disto, a cada dia o volume de informações cresce e se propaga rapidamente e muitas pessoas sentem a necessidade de estarem conectadas e utilizam estes meios de comunicação para a realização das mais diversas atividades.. Estamos vivendo uma era que muitos chamam de "Era da Informação", pois cada um pode ser responsável por produzir e disseminar suas informações para todo o mundo.

Assim uma das grandes preocupações do mundo nos dias de hoje é de como fazer para garantir a segurança da informação no mundo digital, tanto dentro das organizações (pública ou privada), quanto dentro da casa dos cidadãos de forma individual ou coletiva. Além disso, temos uma série de exemplos de ataques a centros ou *sites* onde se tem muita informação em forma de protesto, como por exemplo, ataque de *hackers* chineses ao site da Casa Branca, ficando este site fora do ar por algumas horas (Kelvin, Anderson). Sem falar no caso Edward Snowden onde ele mostrou ao mundo que o Presidente dos EUA tinha acesso a informações sigilosas de outros países conquistadas através de invasões a sistemas (G1 Globo). Por estes e outros motivos, na era do conhecimento em que vivemos, é imprescindível manter a segurança da informação nas organizações, considerada como um ativo que deve ser protegido devido ao seu valor estratégico para a organização.

Segundo TANENBAUM (2003), a segurança é um assunto abrangente e inclui inúmeros tipos de problemas. Por exemplo, a segurança se preocupa em garantir que pessoas mal-intencionadas não leiam ou, pior ainda, modifiquem secretamente mensagens enviadas a outros destinatários. Outra situação é a de evitar que pessoas não autorizadas tenham acesso aos locais onde informações ficam salvas.

Para ajudar a direcionar as organizações a tomar medidas de Segurança da Informação para se protegerem, a norma NBR ISO 27002 foi criada para estabelecer diretrizes e princípios para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização (NBR 270002). Assim é possível manter um processo de segurança da informação normatizado e aderente a padrões internacionais e nacionais, o que traz diversos benefícios às organizações. Apesar de ser uma norma, a NBR/ISO 27002 não tem poder de lei

e serve como um guia de implantação de mecanismos de segurança da informação. Ainda era necessário organizar em forma de lei diversos mecanismos existentes atualmente de salvaguarda de informação com validade legal.

Nesse sentido, o governo Brasileiro resolveu se adiantar a grande maioria dos países do mundo, inclusive países mais desenvolvidos, e decidiu criar depois de algum tempo em debate, inclusive com uma consulta popular no site *culturadigital.br*, o Marco Civil da Internet. Para muitos é chamado de "A Constituição da Internet", onde foram definidos os direitos e deveres e assim auxiliar no uso responsável da rede.

O Marco Civil considera a Internet como uma ferramenta fundamental para a liberdade de expressão e que deve ajudar o brasileiro a se manifestar como quiser de acordo com a Constituição Federal. O texto ainda fala que "o acesso a Internet é fundamental para o exercício da cidadania". Para alcançar esses objetivos, o Marco Civil da Internet foi construído considerando três aspectos: neutralidade da rede, liberdade de expressão e sigilo. (BRASIL,Lei n°2.126).

A neutralidade da rede diz que as operadoras estão proibidas de limitar a velocidade da conexão da rede pelo tipo de uso do usuário ou de vender pacotes de internet pelo tipo de uso, assim a velocidade contratada tem que ser entregue e cada um usa da forma que achar correta.

Já a liberdade de expressão aborda que cada um é responsável pelo seu conteúdo produzido na rede e não mais os provedores de acesso. Assim "o conteúdo postado é de responsabilidade do usuário da conexão e não de quem fornece. Quem oferece serviços, como redes sociais, só pode ser considerado culpado se a justiça mandar retirar a publicação do ar e isso não for feito no prazo estipulado" (Pereira, Leonardo).

Por fim o sigilo garante ao usuário da rede que sua vida privada não será violada. Seus dados só serão repassados se ele autorizar ou por ordem judicial. Com isso os provedores de Internet só podem fornecer informações dos usuários se receberem ordens judiciais. Para atender às demandas da justiça, os dados dos registros de conexão tem que ser guardados por um ano e os registros de acesso a aplicações por seis meses.

O Marco Civil determinou ainda, entre outras coisas, que os registros de conexão dos usuários permaneçam guardados por um determinado tempo em ambiente monitorado e sigiloso, como podemos ver na subseção I do Marco Civil da Internet, que trata 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 um ano, nos termos do regulamento.

O ambiente monitorado tem como objetivo prevenir acessos não autorizados e que essas informações fiquem guardadas em ambientes seguros e protegidas. E sigilosa para que apenas pessoas autorizadas tenham acesso a informação

As empresas estrangeiras que atuam no país tem que adequar a esta nova legislação. Caso descumprir estas normas poderão sofrer sanções, multas, suspensão ou até serem proibidas de cumprir suas atividades. (Pereira,Leonardo)

Considerando as definições e abrangência do Marco Civil e o contexto das Universidades Federais, temos que estas últimas são provedores de acesso aos seus servidores e alunos e assim também estão sujeitas às interpretações do Marco Civil da Internet. Assim é necessário implementar e replicar as exigências do Marco Civil nesse ambiente e para isso o uso de normatizações, como a NBR/ISO 27002, mostra-se uma ferramenta importante no desenvolvimento dessas diretrizes.

Neste contexto, a UFPB oferece acesso a rede para toda a comunidade acadêmica e assim sendo, guardar os registros de acessos dos usuários da rede UFPB torna-se importante. No desenvolvimento deste trabalho está sendo considerado um conjunto mais restrito de redes e sistemas da UFPB, localizado no Campus IV de Rio Tinto, que consiste nos laboratórios dos Cursos de Sistemas de Informação e Licenciatura em Ciências da Computação, por serem laboratórios com as características e permissões de acesso necessárias para estudo, desenvolvimento e validação das propostas deste trabalho.

1.1 Objetivo

1.1.1 Objetivo Geral

Apresentar uma análise e propor a adequação do registro de conexão ao se utilizar os laboratórios do Campus IV destinados aos cursos de SI e LCC de acordo com o Marco Civil da Internet e considerando a NBR 27002 como um guia de procedimentos de registros, sigilo e ambiente controlado.

1.1.2 Objetivos Específicos

- **Objetivo específico 1:** Identificar os principais pontos referentes a Registro de Conexão, Sigilo e Ambiente Controlado no Marco Civil e na NBR27002.
- **Objetivo especifico 2 :** Fazer um paralelo entre os pontos em comum da NBR 27002 e do Marco Civil sobre Registro de Conexão, Sigilo e Ambiente Controlado .
- **Objetivo especifico 3**: Analisar a infra estrutura do laboratório relacionadas ao registro de conexão, sigilo e ambiente controlado, adequando ao Marco Civil da Internet, tendo como guia de implementação a NBR 27002.

1.2 Metodologia

O presente trabalho elabora o desenvolvimento de uma proposta inicial para adequar os Laboratórios de Informática do Campus IV da UFPB ao Marco Civil da Internet e a NBR 27002.

Para verificar a conformidade com o Marco Civil e entender o que propõem a ISO/NBR 27002 foi utilizado uma pesquisa exploratório através de uma Pesquisa Bibliográfica necessária para levantar os assuntos que serão abordados. As etapas desenvolvidas para este processo foram:

- Levantamento Bibliográfico referente ao Marco Civil da Internet;
- Levantamento Bibliográfico referente a NBR 27002;
- Paralelo entre o Marco Civil e a NBR;
- Analise dos Laboratórios de Informática dos Cursos de Sistemas de Informação e Ciências da Computação através de estudos já existentes e conversas informais com o responsável pelos laboratórios;
- Proposta para adequação dos laboratórios a respeito do Sigilo e Ambiente Controlado para a segurança das informações baseado no Marco Civil da Internet.

1.3. Estrutura do Trabalho

No capítulo 1 deste trabalho apresentamos a introdução ao Marco Civil, além dos objetivos gerais, específicos, metodologia e estrutura do trabalho. No capítulo 2 apresentamos a fundamentação teórica onde abordaremos a Segurança da Informação, a NBR, o Marco Civil e seus principais pontos. Além de tratarmos do Sigilo e Ambiente Controlado. No capítulo 3 abordaremos as Ferramentas utilizadas em nossos laboratórios. No Capítulo 4

Teremos um Paralelo entre o Marco Civil e a NBR 27002 além da análise da estrutura dos laboratórios, aspectos como a estrutura Física, de Conectividade e infra estruturas de serviços e alguns cenários de uso. No capitulo 5 trataremos da adequação ao Marco Civil e no Capitulo 6 teremos as conclusões .

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo visa à definição dos principais conceitos teóricos diretamente relacionados com o tema pesquisado. Tais conceitos se referem à Segurança da Informação, Marco Civil da Internet, NBR 27002, Ambiente Controlado e Sigilo.

2.1 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é um tema muito discutido no ambiente organizacional, tanto privado como público, e pelos cidadãos em geral, pois todos estes utilizam muitas informações diariamente, muito mais do que em qualquer época passada da civilização. Assim, é necessária toda uma estrutura para dar suporte a essa troca de informações e além deste suporte é necessário garantir a segurança destas informações.

Segundo a NBR 27002, existem três princípios básicos da segurança da informação para garantir a proteção dos ativos contra ameaças:

- Confidencialidade: As informações devem ser conhecidas apenas pelos indivíduos que detém as permissões de acesso, evitando assim o "vazamento" de informação e dificultando a espionagem industrial;
- Integridade: As informações devem ser mantidas no seu estado original sem alterações, garantindo a quem as receber, a certeza de que não foram falsificadas, corrompidas ou alteradas;
- Disponibilidade: O acesso a todos os dados no momento que for necessário para a utilização.

Ainda de acordo com a NBR 27002, segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (NBR 27002).

A NBR 27002 também diz que a segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

O objetivo fundamental da segurança da informação é proteger o interesse daquelas pessoas que confiam na informação, assim como sistemas e meios de comunicações que fornecem a informação de falhas de disponibilidade, confidencialidade e integridade (COBIT Security Baseline,).

Em Kurose e Ross, encontramos as seguintes definições:

a) Confidencialidade: apenas o remetente e o destinatário pretendido podem entender o conteúdo da mensagem transmitida, que deve estar cifrada de alguma maneira, para que ela não seja decifrada por algum interceptador;

b) Autenticação: o remetente e o destinatário precisam confirmar a identidade da outra parte envolvida na negociação – confirmar se a outra parte é realmente quem alega ser;

c) Integridade: mesmo que o remetente e o destinatário consigam se autenticar reciprocamente, eles também querem assegurar que o conteúdo da comunicação não seja alteado durante a transmissão;

d) Não repúdio: impede que uma entidade (computador, pessoa, etc.) envolvida em uma transação negue sua participação;

e) Disponibilidade: os recursos devem ficar disponíveis para serem usados por seus usuários legítimos;

f) Controle de acesso: limita o acesso de recursos apenas a pessoas autorizadas.

Na prática, a segurança da rede envolve não apenas proteção, mas também detecção de falhas de comunicação seguras e ataques à infraestrutura e reação a esses ataques. E muitos casos, um administração pode implementar mecanismos especiais de proteção para reagir a ataques. Nesse sentido, a segurança de rede é conseguida por meio de um ciclo contínuo de proteção, detecção e reação.(Kurose e Ross)

.

Para colocar os conceitos de segurança da informação apresentados, as organizações devem definir normas e procedimentos específicos. Assim uma série de padronizações surgiram para implementar segurança da informação em ambientes organizacionais. Uma que merece destaque é a NBR 27002, apresentada em maiores detalhes na próxima seção.

2.2 NBR 27002

ABNT NBR ISO / IEC 27002 é o conjunto de normas e boas práticas para a gestão da segurança da informação que especifica quais requisitos devem ser implementados e ajuda na orientação nos controles de segurança das organizações. Sendo assim funciona como um guia para organização desenvolver procedimentos de segurança da informação.

A norma está dividida em 11 seções de controles de segurança da informação. Do capítulo um ao quatro a norma apresenta seu objetivo, termos e definições, além de apresentar

como a norma está estruturada e fala também sobre análise e tratamento de riscos. Nos demais capítulos temos:

- **Políticas de Segurança da Informação** que tem como objetivo, prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.
- **Organizando a Segurança da Informação**, como gerenciar a segurança da informação dentro da organização, convém que uma estrutura de gerenciamento seja estabelecida para iniciar e controlar a implementação da segurança da informação dentro da organização.
- **Gestão de Ativos**, para Alcançar e manter a proteção adequada dos ativos da organização,convém que todos os ativos sejam inventariados e tenham um proprietário responsável.
- **Segurança em Recursos Humanos**, para assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, e reduzir o risco de roubo, fraude ou mau uso de recursos. Convém que as responsabilidades pela segurança da informação sejam atribuídas antes da contratação, de forma adequada, nas descrições de cargos e nos termos e condições de contratação.
- **Segurança Física e do Ambiente,** prevenir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.
- **Gestão das Operações e Comunicações**,garante a operação segura e correta dos recursos de processamento da informação.
- **Controle de Acessos**,Controla acesso à informação, convém que o acesso à informação, recursos de processamento das informações e processos de negócios sejam controlados com base nos requisitos de negócio e segurança da informação.
- **Aquisição, Desenvolvimento e Manutenção de Sistemas**, garante que segurança é parte integrante de sistemas de informação, convém que todos os requisitos de segurança sejam identificados na fase de definição de requisitos de um projeto e justificados, acordados e documentados como parte do caso geral de negócios para um sistema de informações.
- **Gestão de Incidentes de Segurança da Informação,** tem o objetivo de assegurar que fragilidades e eventos de segurança da informação associados

com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

- **Gestão da Continuidade do Negócio**, não permite a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso**.**
- **Conformidade**, evita a violação de qualquer lei criminal ou civil, estatutos, regulamentações ou obrigações contratuais e de quaisquer requisitos de segurança da informação, projeto, a operação, o uso e a gestão de sistemas de informação podem estar sujeitos a requisitos de segurança contratuais, regulamentares ou estatutários. (NBR 27002)

Por ser um ponto chave do sigilo e ambiente controlado do Marco Civil, é necessário uma descrição mais detalhada das subseções que compõe a seção sobre Monitoramento pois tratam especificamente do registro de atividades.

Para isso convém que os sistemas sejam monitorados e eventos de segurança da informação sejam registrados. Os registros (log) de operador e registros (log) de falhas sejam utilizados para assegurar que os problemas de sistemas de informação são identificados. Que as organizações estejam de acordo com todos os requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento. O monitoramento do sistema seja utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.

2.2.1 Registro segundo a NBR27002

Uma atenção especial é dada ao capítulo 10 da NBR 27002 pois trata do Monitoramento. Entre as seções 10.10.1 até a seção 10.10.6 tem-se guias para Registros de Auditoria, Monitoramento, Proteção dos Registros (Logs).

2.2.1.1 Registro de Auditoria.

Registro de auditoria é abordado na seção 10.10.1 da NBR 270002, que contém as atividades dos usuários, exceções e outros eventos de segurança da informação produzidos por e mantidos por um determinado tempo acordado para auxiliar futuras investigações e monitoramento de acesso. Nestes registros de (log) auditoria podem incluir quando relevante:

- identificação dos usuários;
- datas, horários e detalhes de eventos-chave, como, por exemplo log on e log off
- identidade do terminal ou, quando possível, sua localização.

Nestes registros podem conter dados pessoais confidenciais, portanto medidas de proteção de privacidade devem ser tomadas.

A seção 10.10.2 trata do Monitoramento do uso do sistema. Deve ser estabelecidos procedimentos para monitorar o uso dos recursos de processamento da informação e os resultados do monitoramento devem ser analisados criticamente de forma regular. O nível de monitoramento para os recursos requeridos devem ser determinados através de uma análise/avaliação de riscos. A organização deve estar de acordo com todos os requisitos legais relevantes para suas atividades de monitoramento.

O uso de procedimentos de monitoramento do sistema se faz necessário para podermos assegurar que só as atividades que foram autorizadas estão sendo executadas pelos usuários.

Já a seção 10.10.3 fala da Proteção das Informações dos registros (log). As informações de registro (log) e os recursos devem ser protegidos contra acesso não autorizado e falsificação. Os controles implementados devem proteger contra modificação não autorizada e problemas operacionais com os recursos dos registros (log), tais como:

Alterações dos tipos de mensagem que são gravadas ou arquivos de registros (logs) sendo editados ou excluídos.

Alguns registros de auditoria podem ser guardados como parte da política de retenção de registros. Os registros de auditoria de sistemas (log) podem ser guardados como parte política de retenção de registros ou devido aos requisitos para a coleta e retenção e evidências.

Na seção 10.10.4 teremos os Registros (log) de administrador e operador. As atividades dos administradores e operadores dos sistemas devem ser registradas. Nestes registros devem incluir:

- a hora que o evento ocorreu;
- informações sobre o evento
- a conta que o administrador ou operador esta envolvido
- os processos que estavam envolvidos

Os registros de atividades dos operadores e administradores devem ser analisados criticamente em intervalos regulares.

A seção 10.10.5 trata do Registro (log) de Falhas. As falhas ocorridas devem ser registradas e analisadas e ações apropriadas devem ser adotadas as falhas informadas por usuários ou pelos programas devem ser registradas e deve existir regras claras para o tratamento das falhas informadas.

Por fim, a seção 10.10.6 trata da Sincronização dos Relógios. Os relógios de todos os sistemas de processamento de informações consideradas relevantes devem ser sincronizados de forma precisa dentro da organização. O relógio deve ser ajustado conforme foi acordado, segundo um padrão de tempo universal ou local e é importante que exista um procedimento para verificar e corrigir a variação de tempo entre os relógios. Este estabelecimento correto do tempo dos relógios é importante para assim assegurar a exatidão dos registros (log) que podem ser requeridos para investigações.

O Marco Civil determina que as informações de registro de conexão (logs) sejam mantidas sob sigilo e em ambientes controlados. Assim faz-se necessário detalhar essas questões nas próximas seções.

2.3 Marco Civil da Internet

Desde 2007 o Brasil começou a discutir o Marco Civil da Internet e depois de muito tempo o texto final foi apresentado e sancionado pela presidente Dilma Roussef. Ele é tido como um texto pioneiro no mundo pois estabelece algumas regras, direitos e deveres no ambiente virtual brasileiro. O documento é considerado como uma “Constituição da Internet” já que estabelece regras, liberdade de expressão, proteção a privacidade, neutralidade da rede, além de definir as responsabilidades de cada um no ambiente virtual. Ele foi criado e debatido por cerca de 2 mil pessoas que ajudaram a escrever o texto que foi para o congresso, que foi construído sobre três pilares: liberdade, neutralidade e privacidade. (Terra)

2.3.1 Neutralidade da Rede

Com o Marco Civil da Internet o Brasil definiu a neutralidade da rede como regra e isto faz com que os provedores de Internet estejam proibidos de dar mais atenção a um serviço do que pra outros. Em linhas gerais quer dizer que as operadoras estão proibidas de vender pacotes de Internet pelo tipo de uso. Isto faz com que o usuário esteja protegido de ter sua conexão diminuída baseadas em interesses econômicos. Sendo regra, a neutralidade da rede faz com que o servidor tenha que se explicar caso ele discrimine o tráfego na rede. A rede deve ser igual para todos, assim ele impede que empresas cobre valores diferentes pelo que você acessa Internet, todo

mundo paga a mesma coisa e acessa o que quiser, claro que de acordo com o valor e velocidade contratada com o provedor.

2.3.2 Liberdade de Expressão

A Lei regula o monitoramento, filtragem, análise e fiscalização de conteúdo para que assim possa garantir o total direito a privacidade, garantindo a possibilidade de produção, acesso e compartilhamento de qualquer tipo de conteúdo. Com isso, a partir de agora as empresas que fornecem a conexão não serão responsabilizadas pelo conteúdo postado pelos usuários, a não ser que a justiça considere o conteúdo impróprio e a partir daí ordenar que se retire o material do ar e o mesmo não seja feito pela empresa. Ainda na questão de liberdade de expressão, só a justiça, por meio de ordens judiciais para fins investigativos, que pode ter acesso ao conteúdo dos usuários. As empresas que não cumprirem as leis que dizem respeito a privacidade na Internet poderão ser penalizadas com multa, advertência, chegando até a proibição de suas atividades, ainda podendo receber penalidades administrativas, cíveis e criminais.

2.3.3 Privacidade dos Usuários

O respeito a privacidade é um dos princípios fundamentais do uso da Internet no Brasil. No artigo 7º do Marco Civil entre um dos vários direitos dos usuários, se trata do direito a inviolabilidade da intimidade e da vida privada, assegurando assim seu direito a proteção e indenização pelos danos morais decorrente da sua violação. Também se fala do direito a inviolabilidade e ao sigilo de suas comunicações, salvo por ordem judicial, com isso o usuário passa a ter o direito de não ter seus dados de conexão repassados pra outras pessoas sem seu consentimento. Hoje algumas empresas trabalham com esse tipo de dado sem nenhuma regulamentação, causando insegurança jurídica para ambas as partes. A proteção dos dados também é garantida no Marco Civil, no artigo 8º é dito que a garantido direito a privacidade e a liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet . E no parágrafo 3º do artigo 9º é dito que é vedado bloquear, monitorar, filtrar ou analisar conteúdo dos pacotes de dados. (Molon, Alessandro)

2.3.4 Guarda de Registros (*Logs)*

Log pode ser utilizado como abreviação da palavra *Logging* e está definido na NBR 27002 como sendo “um processo de estocagem de informações sobre eventos que ocorreram em um *firewall* ou em uma rede”, e se da através de dados obtidos por de registros de acessos gerados

pelos usuários e nestas informações podem conter o endereço IP da máquina, a hora e data de acesso dos usuários e seus respectivos acessos na rede.

"Conforme determinado no Marco Civil da Internet, o provedor de conexão só pode guardar os *registros* de conexão do usuário (e não os de acesso a aplicações) e apenas pelo prazo de um ano. O prazo só pode ser estendido mediante decisão judicial, para auxiliar em uma investigação. O provedor de conexão, portanto, não poderá armazenar informações sobre o que você anda buscando na Internet e o que escreve por aí, pois lhe é vedado guardar os registros de aplicação. Assim, sua privacidade está mantida. Por sua vez, os provedores de aplicações, como UOL, Facebook, Google, YouTube, Skype, os blogs e páginas da Internet em geral, podem guardar apenas os registros de aplicação – ou seja, os registros de acesso às suas aplicações ou serviços, para identificar quando um usuário as acessa". (Molon,Alessandro.)

No Marco Civil da Internet, registro de Conexão é definido como: "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;

Além das premissas básicas de liberdade de expressão, neutralidade, etc. o Marco Civil também aborda e influencia outras questões relacionadas à Internet no Brasil, como a disciplina do uso da Internet no Brasil que tem como fundamentos além do respeito à liberdade de expressão, como o desenvolvimento da personalidade e o exercício da cidadania através de meios digitais, a abertura e a colaboração, também a livre concorrência e a defesa do consumidor. O texto também fala que a disciplina do uso da Internet no Brasil tem como objetivos de promover o acesso a Internet a todos, promover o acesso a informação, ao conhecimento, ao conhecimento e a participação na vida cultural e na condução dos assuntos públicos, como também promover a inovação e a difusão de novas tecnologias.

2.4 Sigilo

O Marco Civil da Internet diz que os registros de conexão devem ser guardados em ambientes controlados e em sigilo. Sigilo é um sinônimo de confidencialidade e é este último que iremos utilizar neste trabalho.

Segundo Sêmola, confidencialidade é a propriedade da informação em que estar a salvo de acesso e divulgação não autorizadas. Em outras palavras, sua preservação é a garantia do resguardo das informações dadas pessoalmente em confiança e proteção contra sua revelação não autorizada. (Sêmola)

Já para Kurose e Ross, confidencialidade é quando somente o remetente e o destinatário pretendido devem poder entender o conteúdo da mensagem transmitida. (KUROSE E ROSS).

A NBR 27002 fala sobre acordos de confidencialidade e segundo ela convém que os requisitos para confidencialidade ou acordos de não divulgação reflitam a necessidade da organização para proteção da informação devem ser bem analisados e de forma regular. Esses acordos devem considerar requisitos para proteger a informação usando termos obrigados por lei e devem ser considerados os seguintes aspectos:

- A definição de informação a ser protegida, como por exemplo, informação confidencial.
- O tempo de duração deve ser acordado e incluir situações onde a confidencialidade tenha que ser mantida indefinidamente.
- As responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação, também o uso permitido da informação confidencial e os direitos do signatário para usar informação, o direito de auditar e monitorar as atividades que envolvem as informações confidenciais e algumas ações esperadas a serem tomadas no caso de uma violação deste acordo (NBR 27002).

A norma também diz que acordos de confidencialidade e de não divulgação protegem as informações da organização e informam aos signatários das suas responsabilidades para proteger, usar e divulgar a informação de maneira responsável e autorizada. E pode haver a necessidade de uma organização usar diferentes formas de acordos de confidencialidade ou de não divulgação em diferentes circunstancias (NBR 27002).

2.5 Ambiente Controlado

Segundo Moura e Gaspary (2008), a proteção da informação é conseguida através da aplicação de segurança física e lógica nas operações das empresas, e o que orienta essas práticas nas organizações são as Políticas de Segurança da Informação que, conforme Marciano (2006), abrangem recursos computacionais, recursos humanos, infra estrutura e logística.

Segundo Silva, P. T.; Botelho, Hugo; Torres, C. B., o ambiente físico no qual a organização faz suas operações pode constituir um dos mais importantes elementos no que diz respeito à salvaguarda da informação. A definição de áreas na organização contribui para a construção de ambientes seguros, mas existem erros que são frutos de condicionamento destes espaços e estes erros podem fragilizar a capacidade de proteção da informação. Por exemplo,

componentes críticos de armazenamento, processamento ou transmissão não deverão encontrar-se demasiado expostos, nem deverão ser de acesso demasiado fácil (Silva, P. T.; Botelho, Hugo; Torres, C. B.).

Outro aspecto importante também abordado pelos autores é sobre o controle de quem entra e de quem sai das instalações, pois é um aspecto particularmente importante da segurança física. Para eles não basta ter um guarda à entrada e obrigar todos os visitantes a registrarem-se. É fundamental ter a certeza, por exemplo, de que os visitantes não levam material da empresa sem autorização expressa do responsável por esse equipamento. Vale salientar que o "controle de acesso não se resume a uma portaria com guardas e, eventualmente, um sistema de vídeo em circuito fechado. Este controlo deve ser alargado a todas as áreas sensíveis, nomeadamente aos centros de dados e aos arquivos centrais, e deverá ser abrangente na medida em que não devem existir exceções." (Silva,P.T; Botelho,Hugo; Torres, C.B)

A norma NBR 27002 tem um capítulo que trata exclusivamente da Segurança Física e do Ambiente, deixando claro que a segurança da informação se preocupa tanto com a segurança física das áreas quando com a segurança lógica dos equipamentos, tendo assim como objetivos de prevenir acessos não autorizados, danos nas instalações e prevenção de perdas de dados, furtos, roubos de informações das organizações.

A norma diz que as áreas que guardem as informações devem ser devem ser seguras, protegidas por perímetros de segurança definidos (barreiras como portões de entrada com cartão ou balcões de recepção) e controles de acesso apropriados e que o acesso a estas áreas seguras devem ser controladas e só pessoas autorizadas podem ter acesso a estes ambientes, e para isso desse ser estabelecido alguns aspectos como a data e hora da entrada e saída dos visitantes devem ser registradas, o acesso as áreas onde são processadas ou armazenadas as informações devem ser controladas e restrito a pessoas autorizadas, os funcionários e visitantes devem ter alguma forma visível de identificação, os direitos de acesso a áreas seguras devem ser revistos e atualizados em intervalos regulares (NBR 27002).

A norma também fala que sejam projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem publica e outras formas de desastres naturais ou causados pelo homem. E nela deve ser levadas em consideração todas as ameaças a segurança representadas por instalações vizinhas, por exemplo , um incêndio em um edifício vizinho vazamento de água do telhado ou em pisos do subsolo ou uma explosão na rua (NBR 27002).

Para o trabalho em áreas seguras a norma diz que convém que seja projetada e aplicada proteção física, bem como diretrizes para o trabalho em áreas seguras. E para isto devem ser levadas em consideração algumas diretrizes como que o pessoal só tenha conhecimento da existência de áreas seguras ou das atividades nelas realizadas, apenas se for necessário, que seja evitado o trabalho não supervisionado em áreas seguras, tanto por motivos de segurança como para prevenir as atividades mal intencionadas, quando não ocupadas as áreas seguras devem ser fisicamente trancadas e periodicamente verificadas e que não seja permitido o uso de maquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos moveis, salvo se for autorizado. (NBR 27002).

2.6. Considerações Finais

Neste capítulo podemos aprofundar o conhecimento em alguns assuntos que são a base deste trabalho, como os conceitos de Segurança da Informação. O que diz a NBR 27002 que trata da implantação da Segurança da Informação nas organizações como o que diz o Marco Civil, sobre os direitos e deveres dos cidadãos e como se deve agir para estar de acordo com a lei. Tratamos do Sigilo e do Ambiente Controlado.

Em seguida, abordaremos algumas ferramentas que são utilizadas em nossos laboratórios para auxiliar os administradores dos laboratórios no controle do acesso a rede.

3.0. Ferramentas Utilizadas no Laboratório

Neste Capitulo descreveremos algumas ferramentas e suas formas de controle utilizadas na rede dos laboratórios de Informática.

3.1 PfSense

O PfSense é “um sistema operacional de código aberto usado para transformar o computador e um *firewall*, roteador. Ele é baseado no projeto *monowall*, uma distribuição poderosa e leve” (Persaud, Chistopher). Ele pode ser instalado em pequenas redes domestica protegendo apenas um único computador ou nas grandes organizações protegendo muitos computadores. Ele é a evolução do firewall tradicional, pois une vários serviços como vpn, balanceamento de carga, regras de firewall, monitoramento de trafego, etc.

NAKAMURA e GEUS define o firewall como sendo “um ponto entre duas ou mais redes, que pode ser um componente ou conjunto de componentes, por onde passa todo o tráfego, permitindo que o controle, a autenticação e os registros de todo o tráfego sejam realizados. (NAKAMURA e GEUS)

Existe dois tipos de funcionamento básico do firewall, um que é baseado na filtragem de pacotes e outro que é baseado no controle de aplicações e cada um trabalha para um

determinado fim. Na filtragem de pacotes por meio de regras estabelecidas ele determinada quais endereços IP's e dados podem estabelecer comunicação, transmitindo ou recebendo dados. Alguns sistemas ou serviços podem ser liberados ou bloqueados. Já o firewall de aplicação permite que os responsáveis pela administração da rede possa ter um acompanhamento mais preciso do trafego na rede, contando inclusive com ferramentas de auditoria, eles são conhecidos como Proxy e não permite a comunicação direta entre a rede e a internet tudo passa pelo firewall que funcionar como o intermediador. O Proxy efetua a comunicação entre ambos por meio do numero de sessão TCP dos pacotes.

3.2 Squid

O servidor Squid Web Proxy Cache é gratuito e funciona em código aberto para Unix e Linux. Ele permite que os administradores implementem um serviço de *proxy caching* para Web, acrescentem controles de acesso (regras), e armazenem até mesmo consultas de DNS.

O Squid originou-se de um programa desenvolvido pelo projeto *Harvest* chamado *cached* (*Cache Daemon*). A *National Science Foundation* (NSF) financia o desenvolvimento do Squid através do *National Laboratory of Network Research* (NLANR).

O Squid é um *Web proxy cache* que atende à especificação HTTP 1.1. É utilizado somente por clientes proxy, tais como navegadores Web que acessem à Internet utilizando HTTP, Gopher e FTP. Além disso, ele não trabalha com a maioria dos protocolos Internet. Isto significa que ele não pode ser utilizado com protocolos que suportem aplicativos como vídeo conferência, *newsgroups*, *Real Áudio*, dentre outros. O principal motivo destas limitações é que o Squid não é compatível com programas que utilizem UDP, utilizando este protocolo somente para comunicação inter-cache.(Aurelio, Marcos)

O *Squid* registra todos os pedidos de conexão de aplicação web em um arquivo de registro do próprio Squid. A figura 1 mostra o Squid capturando os Ip's que estão conectados a rede, neste exemplo ele tem um processo para atualizar-se a cada 3 segundos para identificar os Ip's que estão ativos ou não.

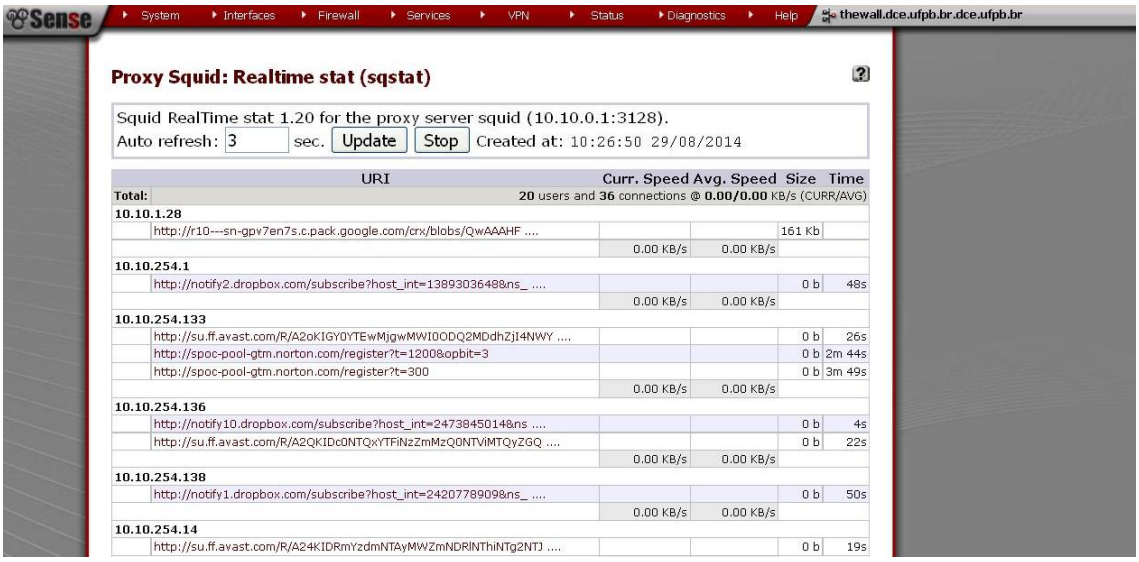
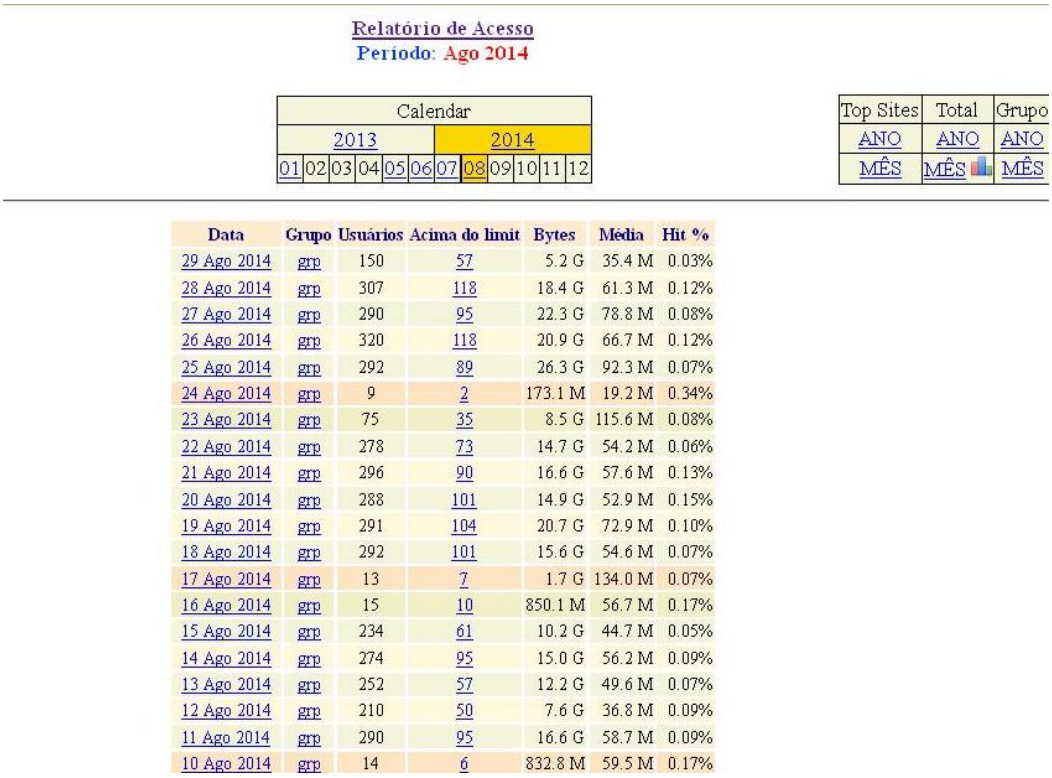


Figura 1- Captura de Ip pelo Squid

3.3 Light Squid

O Light Squid é um analisador de registro do Squid que gera relatórios diários dos acessos dos usuários à Internet e armazena estas informações. A figura 2 apresenta um exemplo de um relatório do LightSquid .

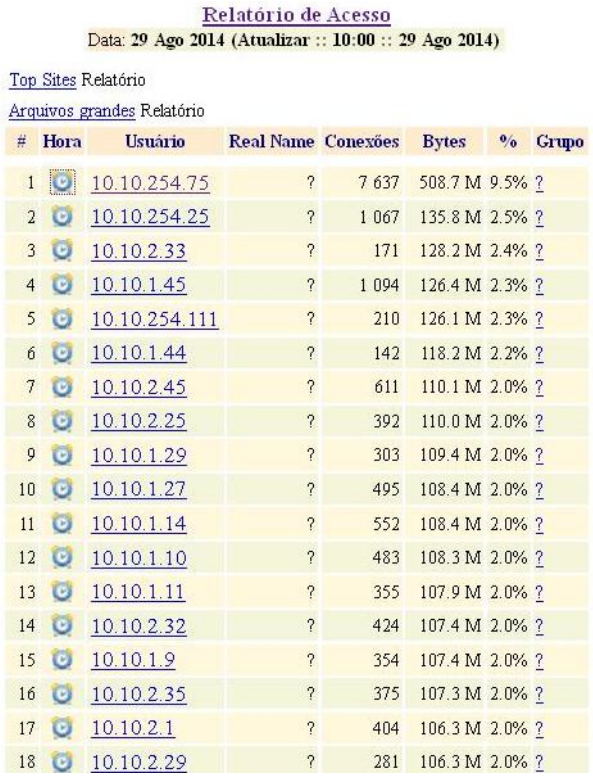


Data	Grupo	Usuários	Acima do limit	Bytes	Média	Hit %
29 Ago 2014	grp	150	57	5.2 G	35.4 M	0.03%
28 Ago 2014	grp	307	118	18.4 G	61.3 M	0.12%
27 Ago 2014	grp	290	95	22.3 G	78.8 M	0.08%
26 Ago 2014	grp	320	118	20.9 G	66.7 M	0.12%
25 Ago 2014	grp	292	89	26.3 G	92.3 M	0.07%
24 Ago 2014	grp	9	2	173.1 M	19.2 M	0.34%
23 Ago 2014	grp	75	35	8.5 G	115.6 M	0.08%
22 Ago 2014	grp	278	73	14.7 G	54.2 M	0.06%
21 Ago 2014	grp	296	90	16.6 G	57.6 M	0.13%
20 Ago 2014	grp	288	101	14.9 G	52.9 M	0.15%
19 Ago 2014	grp	291	104	20.7 G	72.9 M	0.10%
18 Ago 2014	grp	292	101	15.6 G	54.6 M	0.07%
17 Ago 2014	grp	13	7	1.7 G	134.0 M	0.07%
16 Ago 2014	grp	15	10	850.1 M	56.7 M	0.17%
15 Ago 2014	grp	234	61	10.2 G	44.7 M	0.05%
14 Ago 2014	grp	274	95	15.0 G	56.2 M	0.09%
13 Ago 2014	grp	252	57	12.2 G	49.6 M	0.07%
12 Ago 2014	grp	210	50	7.6 G	36.8 M	0.09%
11 Ago 2014	grp	290	95	16.6 G	58.7 M	0.09%
10 Ago 2014	grp	14	6	832.8 M	59.5 M	0.17%

Figura 2 – Relatório de Acessos no Light Squid

Podemos analisar os registros através da escolha do ano, mês e a data desejada, ele mostra o grupo, a quantidade de usuários, a quantidade de bytes trafegados na data solicitada e a média da bytes trafegados.

Já na figura 3 vemos um relatório de acessos, da data 29 de agosto de 2014, esse relatório de acesso gera outros dois tipos de relatórios. O top sites que mostra os sites acessados por determinado IP e o relatório de Arquivos Grandes que trás uma análise mais completa.



Relatório de Acesso

Data: 29 Ago 2014 (Atualizar :: 10:00 :: 29 Ago 2014)

Top Sites Relatório

Arquivos grandes Relatório

#	Hora	Usuário	Real Name	Conexões	Bytes	%	Grupo
1		10.10.254.75	?	7 637	508.7 M	9.5%	?
2		10.10.254.25	?	1 067	135.8 M	2.5%	?
3		10.10.2.33	?	171	128.2 M	2.4%	?
4		10.10.1.45	?	1 094	126.4 M	2.3%	?
5		10.10.254.111	?	210	126.1 M	2.3%	?
6		10.10.1.44	?	142	118.2 M	2.2%	?
7		10.10.2.45	?	611	110.1 M	2.0%	?
8		10.10.2.25	?	392	110.0 M	2.0%	?
9		10.10.1.29	?	303	109.4 M	2.0%	?
10		10.10.1.27	?	495	108.4 M	2.0%	?
11		10.10.1.14	?	552	108.4 M	2.0%	?
12		10.10.1.10	?	483	108.3 M	2.0%	?
13		10.10.1.11	?	355	107.9 M	2.0%	?
14		10.10.2.32	?	424	107.4 M	2.0%	?
15		10.10.1.9	?	354	107.4 M	2.0%	?
16		10.10.2.35	?	375	107.3 M	2.0%	?
17		10.10.2.1	?	404	106.3 M	2.0%	?
18		10.10.2.29	?	281	106.3 M	2.0%	?

Figura 3- Acessos do dia 29 de Agosto de 2014

Já na figura 4 podemos ver uma lista de classificação de sites, chamada de “Top Site”, que é a lista dos sites acessados pelo IP 10.10.254.75, de acordo com o que temos implantando em nossos laboratórios não podemos identificar quem é o usuário que esta utilizando este IP.

Relatório de Acesso

Usuário: 10.10.254.75 (?)

Grupo: ?

Data: 29 Ago 2014

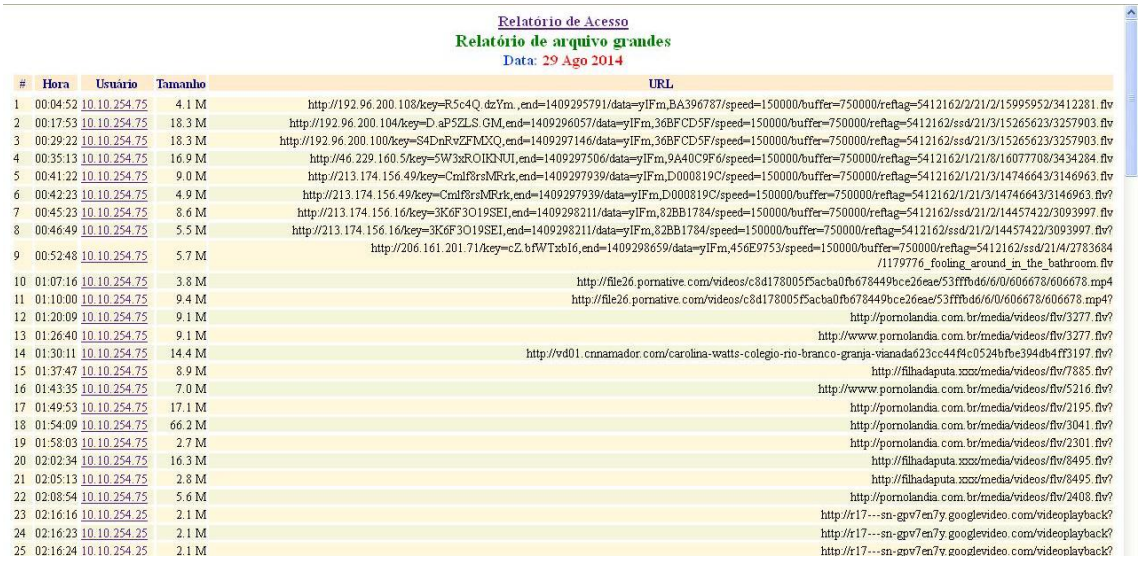
User download "Big Files"

Total 508.7 M

#	Sites acessados	Conexões	Bytes	Soma	%
1	pornolandia.com.br	146	119.0 M	119.0 M	23.4%
2	bg.v4.a.dl.ws.microsoft.com	1 606	90.5 M	209.6 M	17.7%
3	au.v4.download.windowsupdate.com	1 035	48.5 M	258.1 M	9.5%
4	filhadaputa.xxx	41	37.0 M	295.1 M	7.2%
5	www.pornolandia.com.br	467	19.7 M	314.8 M	3.8%
6	46.229.160.5	3	19.2 M	334.0 M	3.7%
7	192.96.200.100	1	18.3 M	352.3 M	3.5%
8	192.96.200.104	1	18.3 M	370.6 M	3.5%
9	213.174.156.16	3	15.2 M	385.7 M	2.9%
10	vd01.cnnamador.com	5	14.5 M	400.2 M	2.8%
11	213.174.156.49	2	13.9 M	414.1 M	2.7%
12	file26.pornative.com	6	13.4 M	427.6 M	2.6%
13	data.ero-advertising.com	100	11.4 M	439.0 M	2.2%
14	contents4127.h2porn.com	1	11.4 M	450.4 M	2.2%
15	bg4.v4.a.dl.ws.microsoft.com	169	8.7 M	459.1 M	1.7%
16	206.161.201.71	1	5.7 M	464.8 M	1.1%
17	192.96.200.108	3	5.4 M	470.2 M	1.0%
18	www.naoconto.com	145	4.0 M	474.2 M	0.7%
19	graphics.pop6.com	34	3.2 M	477.4 M	0.6%

Figura 4 Lista dos Sites Acessados

Ainda podemos ver na figura 5 um exemplo do Relatório de Arquivos Grandes que mostra o IP conectado, neste caso temos o IP 10.10.254.75, à hora e a URL que ele acessou cada site. Para sabermos á hora do primeiro acesso ao último temos que análisar à hora do primeiro e do último acesso e analisar se o IP é o mesmo.



Relatório de Acesso

Relatório de arquivo grandes

Data: 29 Ago 2014

#	Hora	Usuário	Tamanho	URL
1	00:04:52	10.10.254.75	4.1 M	http://192.96.200.108/key=R5c4Q.dzYm.,end=1409295791/data=ylFm,BA396787/speed=150000/buffer=750000/reftag=5412162/2/21/2/15995952/3412281.flv
2	00:17:53	10.10.254.75	18.3 M	http://192.96.200.104/key=D.aP5ZLS.GM,end=1409296057/data=ylFm,36BFCD5F/speed=150000/buffer=750000/reftag=5412162/ssd/21/3/15265623/3257903.flv
3	00:29:22	10.10.254.75	18.3 M	http://192.96.200.100/key=S4DnRvZFMXQ,end=1409297146/data=ylFm,36BFCD5F/speed=150000/buffer=750000/reftag=5412162/ssd/21/3/15265623/3257903.flv
4	00:35:13	10.10.254.75	16.9 M	http://46.229.160.5/key=5W3xROIKNUI,end=1409297506/data=ylFm,9A40C9F6/speed=150000/buffer=750000/reftag=5412162/1/21/8/16077708/3434284.flv
5	00:41:22	10.10.254.75	9.0 M	http://213.174.156.49/key=CmIf8rsMRrk,end=1409297939/data=ylFm,D000819C/speed=150000/buffer=750000/reftag=5412162/1/21/3/14746643/3146963.flv
6	00:42:23	10.10.254.75	4.9 M	http://213.174.156.49/key=CmIf8rsMRrk,end=1409297939/data=ylFm,D000819C/speed=150000/buffer=750000/reftag=5412162/1/21/3/14746643/3146963.flv?
7	00:45:23	10.10.254.75	8.6 M	http://213.174.156.16/key=3K6F3O19SEI,end=1409298211/data=ylFm,82BB1784/speed=150000/buffer=750000/reftag=5412162/ssd/21/2/14457422/3093997.flv
8	00:46:49	10.10.254.75	5.5 M	http://213.174.156.16/key=3K6F3O19SEI,end=1409298211/data=ylFm,82BB1784/speed=150000/buffer=750000/reftag=5412162/ssd/21/2/14457422/3093997.flv?
9	00:52:48	10.10.254.75	5.7 M	http://206.161.201.71/key=cZ.bfWTxbI6,end=1409298659/data=ylFm,456E9753/speed=150000/buffer=750000/reftag=5412162/ssd/21/4/2783684/1179776_fooling_around_in_the_bathroom.flv
10	01:07:16	10.10.254.75	3.8 M	http://file26.pornative.com/videos/c8d178005f5acba0fb678449bce26eae/53fffbd6/6/0/606678/606678.mp4
11	01:10:00	10.10.254.75	9.4 M	http://file26.pornative.com/videos/c8d178005f5acba0fb678449bce26eae/53fffbd6/6/0/606678/606678.mp4?
12	01:20:09	10.10.254.75	9.1 M	http://pornolandia.com.br/media/videos/flv/3277.flv?
13	01:26:40	10.10.254.75	9.1 M	http://www.pornolandia.com.br/media/videos/flv/3277.flv?
14	01:30:11	10.10.254.75	14.4 M	http://vd01.cnnamador.com/carolina-watts-colegio-rio-branco-granja-vianada623cc44f4c0524bfbe394db4ff3197.flv?
15	01:37:47	10.10.254.75	8.9 M	http://filhadaputa.xxx/media/videos/flv/7885.flv?
16	01:43:35	10.10.254.75	7.0 M	http://www.pornolandia.com.br/media/videos/flv/5216.flv?
17	01:49:53	10.10.254.75	17.1 M	http://pornolandia.com.br/media/videos/flv/2195.flv?
18	01:54:09	10.10.254.75	66.2 M	http://pornolandia.com.br/media/videos/flv/3041.flv?
19	01:58:03	10.10.254.75	2.7 M	http://pornolandia.com.br/media/videos/flv/2301.flv?
20	02:02:34	10.10.254.75	16.3 M	http://filhadaputa.xxx/media/videos/flv/8495.flv?
21	02:05:13	10.10.254.75	2.8 M	http://filhadaputa.xxx/media/videos/flv/8495.flv?
22	02:08:54	10.10.254.75	5.6 M	http://pornolandia.com.br/media/videos/flv/2408.flv?
23	02:16:16	10.10.254.25	2.1 M	http://r17---sn-gpv7en7y.googlevideo.com/videoplayback?
24	02:16:23	10.10.254.25	2.1 M	http://r17---sn-gpv7en7y.googlevideo.com/videoplayback?
25	02:16:24	10.10.254.25	2.1 M	http://r17---sn-gpv7en7y.googlevideo.com/videoplayback?

Figura 5- Relatório de Arquivos Grandes

3.4 LDAP

Lightweight Directory Access Protocol (LDAD) "é um protocolo de padrão aberto e multi plataforma muito usado em empresas nos serviços de autenticação e autorização a

sistemas operacionais e aplicativos. Podemos imaginar um servidor LDAP como um banco de dados, mas um banco de dados que não tem SQL, transação, commit e etc. e que os dados são organizados na forma de árvore (igual à árvore genealógica ou a árvore de diretórios que você tem no seu computador) dessa forma os dados podem ser organizados e agrupados mais facilmente". (Furutani, Roberto)

3.5 Samba 4

O Samba é um servidor, é um conjunto de ferramentas que permite que máquinas Linux e Windows se comuniquem e compartilhem arquivos e impressoras. Com ele, é possível construir a topologia de domínios, fazer controle de acesso, compartilhamento, serviço de WINS e outros. (Uira). Ele emula o serviço de Controlador de Domínio da Microsoft (Microsoft Active Directory) que permite gerenciar o parque computacional de computadores, usuários e serviços do ambiente Windows de maneira centralizada.

O modelo de Controlador de Domínio permite um melhor controle sobre usuários e recursos disponíveis em uma rede de computadores de maneira que é possível atender aos requisitos de registro conexões, sigilo e ambiente controlado propostos pelo Marco Civil da Internet, além de dar suporte a implementação dessas soluções de acordo com as especificações da NBR 27002.

4 Análise dos Laboratórios de Acordo com o Marco Civil e a NBR 27002

Analisando o Marco Civil da Internet e a NBR 27002 vemos a possibilidades de associar seus pontos em comum e nos adequar ao Marco Civil que esta em vigor desde o dia 23 de junho de 2014. A UFPB fornece Internet seu corpo docente, discente e servidores, então ela pode ser considerada um provedor de acesso. A partir daí surge a necessidade de gerenciar o acesso a Internet e proteger seus dados e informações, sendo necessário a aplicação do Marco Civil da Internet, pois segundo o 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." (BRASIL,Lei n°2.126).

Assim o presente trabalho pretende associar o Marco Civil da Internet e a NBR 27002 para adequar os laboratórios de informática da UFPB CAMPUS IV a esta nova realidade e assim ter um maior controle sobre os registros (*logs)* de seus estudantes, mas sem esquecer de preservar sua privacidade.

Este capítulo trata da aplicação da norma NBR 27002 considerando agora a existência do Marco Civil da Internet. Especificamente neste trabalho será abordado a questão dos registros de conexão, que é uma exigência do Marco Civil e que é também abordado de acordo com a ISO 27002. Assim, a partir da aprovação do Marco Civil, este se faz presente como lei nos ambientes de rede que provem serviços de acesso. Porém a utilização da NBR traz uma maneira de se aplicar os princípios legais do Marco Civil de maneira a manter aderência a normatizações consolidadas e padronizadas, facilitando auditorias, sistemas de análise, comparação entre sistemas, métricas e indicadores, etc.

Para que o gerenciamento de registros seja implementado de acordo com o Marco Civil e a NBR 27002, algumas abordagens devem ser consideradas, como por exemplo a forma de armazenar os registros de conexão dos usuários dos laboratórios de maneira sigilosa e em ambiente controlado. Para isso, a estrutura atual de funcionamento e uso dos laboratórios foi analisada, considerando-se a política atualmente em vigor no que diz respeito ao modelo de acesso dos usuários e uso dos laboratórios. A partir da análise, foram identificados os problemas relacionados ao registro dos acessos, bem como questões de sigilo e ambiente controlado na guarda dessas informações.

. Antes de a análise ser realizada faz-se necessário uma e correlação dos aspectos abordados no Marco Civil e dos abordados pela NBR27002.

4.1 Pontos em Comum da NBR 27002 e do Marco Civil

Para entendermos melhor a relação entre Marco Civil e NBR 27002, foi realizada uma análise destes dois textos para identificar alguns dos pontos em comum quando se trata a questão da política de registro e do armazenando em ambiente controlado e de forma sigilosa.

A tabela 1 apresenta os pontos em comum da NBR 27002 e do Marco Civil onde a primeira coluna trata dos parágrafos referentes à norma que abordam registros e ambiente controlado e a sessão da norma é especificada no final de cada descrição. Já a segunda coluna informa os artigos da lei do Marco Civil que correspondem ou são semelhantes a norma NBR 27002.

NBR 27002	Marco Civil da Internet
Convém que registros *(log)* de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso. (ver 10.10.1)	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 um ano, nos termos do regulamento.
Os registros (*log*) de auditoria podem conter dados pessoais confidenciais e de intrusos. Convém que medidas apropriadas de proteção de privacidade sejam tomadas (ver 15.1.4).	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, vida privada, honra e imagem das partes direta ou indiretamente envolvidas.
Quando possível, convém que administradores de sistemas não tenham permissão de exclusão ou desativação dos registros (*log*) de suas próprias atividades (ver 10.1.3).	§ 3º O disposto no caput não impede o acesso, pelas autoridades administrativas que detenham competência legal para a sua requisição, aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei.
Convém que sejam estabelecidos procedimentos para o monitoramento do uso dos recursos de processamento da informação e os resultados das atividades de monitoramento sejam analisados criticamente, de forma regular.(ver 10.10.2)	§ 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 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 artigo 7º.
Convém que a organização esteja de acordo com todos os requisitos legais relevantes, aplicáveis para suas atividades de monitoramento.(ver 10.10.2)	§ 4º As medidas e procedimentos de segurança e 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.
O uso de procedimentos de monitoramento é necessário para assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas.(ver 10.10.2) A análise crítica dos registros (*log*) envolve a compreensão das ameaças encontradas no sistema e a maneira pela qual isto pode acontecer(10.10.2)	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.

Tabela 1 – Paralelo entre Marco Civil e ISO 27002

Como já foi mostrado anteriormente o Marco Civil da Internet tem como objetivo "estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil". Enquanto isso a Norma NBR ISO/IEC 27002 é o Código de Prática para a Gestão de Segurança da Informação e tem como objetivo "estabelecer diretrizes e princípios gerais para iniciar,implementar, manter e melhorar a gestão de segurança da informação em uma organização".

Esses dois textos apresentam algumas semelhanças e pontos de acordo, como por exemplo, em ambos os textos os registros de *acesso* contendo atividades dos usuários devem ser mantidos por um determinado tempo para investigação. Esse tempo é definido apenas no Marco Civil da Internet, que diz que o tempo passa a ser de 6 meses a 1 ano.

Outro pronto no qual o Marco Civil e a NBR convergem é sobre o respeito e os direitos dos usuários a partir do armazenamento de suas informações . Para preservar estes direitos é necessário preservar o local onde as informações destes usuários estão registradas e quem são as pessoas que podem ter acesso a este local e a estas informações, por isso ambos falam em ambientes seguros e controlados e a NBR 27002 contém uma série de especificações de como implementar esse tipo de controle.

Assim vemos que estes textos apresentam algumas diretrizes: o Marco Civil vai tratar da relação dos usuários com a Internet, assegurando seus direitos, deveres e responsabilidades, enquanto a NBR ISO/IEC 27002 mostrar como implementar controles para melhorar a segurança da informação.

Para validar uma proposta de implementação do Marco Civil da Internet usando a ISO como normatizadora dos procedimentos de segurança da informação, as próximas seções tratam da análise dos laboratórios de informática, de sua estrutura física, do funcionamento e das tecnologias implantadas nos mesmos.

4.2 Análise dos Laboratórios

4.2.1 – Infra Estrutura Física e de Conectividade

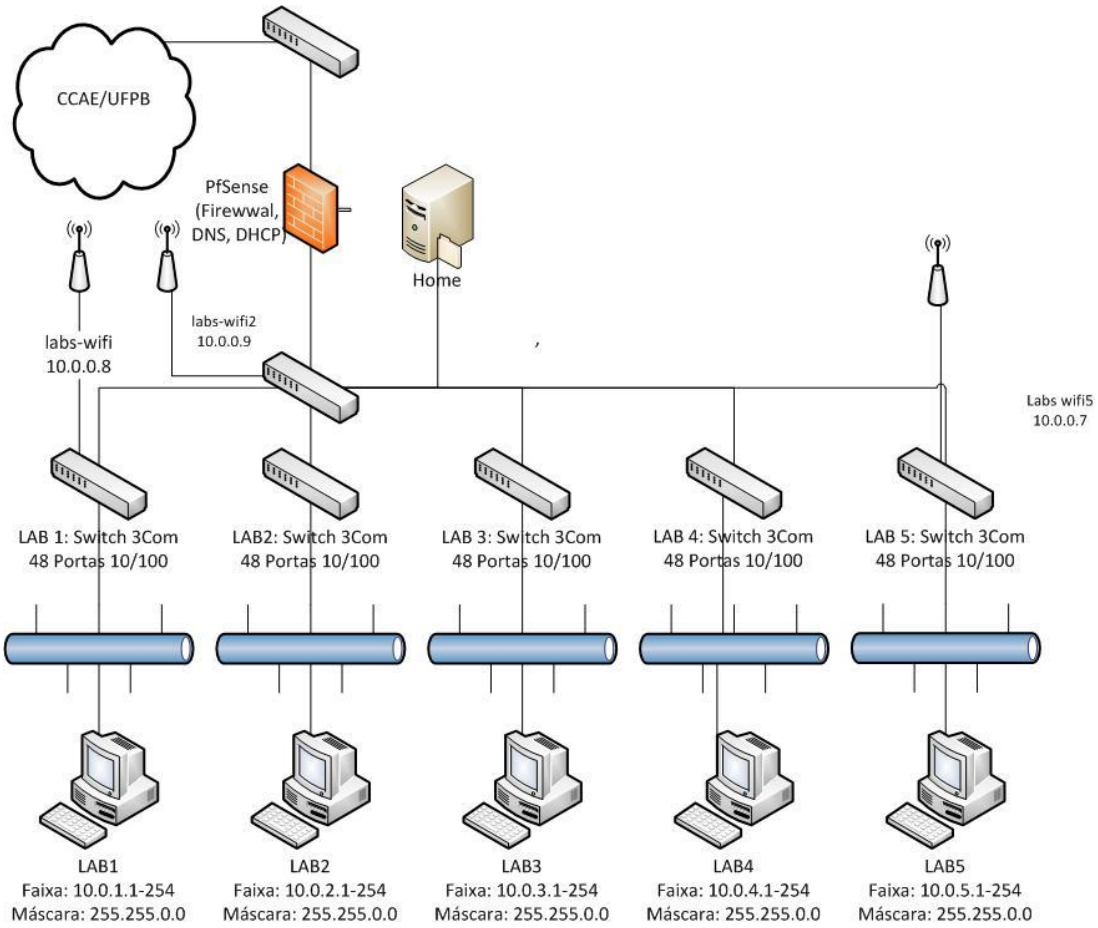
O Curso de Bacharelado em Sistemas de Informação do Campus IV da UFPB conta atualmente com 5 laboratórios de Informática, denominados de Laboratório 1, Laboratório 2, Laboratório 3, Laboratório 4 e Laboratório 5, onde apenas os Laboratórios 1, 2 e 5 são utilizados pelos alunos e professores para aulas e pesquisas. O laboratório 1 conta com 48 máquinas em funcionamento, o laboratório 2 conta com 45 máquinas em funcionamento e o laboratório 5 conta com 24 máquinas em funcionamento. .

Para ter acesso aos laboratórios e ter acesso aos recursos disponíveis é necessário estar presente durante seu horário de funcionamento, acompanhado de um responsável que pode ser um professor, um monitor de disciplina ou ter obtido uma autorização especial da coordenação para ter acesso aos mesmos.

O endereçamento IP da rede dos laboratórios é 10.0.0.0/16, onde se utiliza da máscara de rede de 16 bits. A rede é abrangente, mas logicamente os laboratórios são associados através de uma nomenclatura associada ao número do laboratório, por exemplo, o Laboratório 1 possui máquinas na rede 10.0.1.0/16, enquanto que o Laboratório 2 tem máquinas na rede 10.0.2.0/16, e assim sucessivamente nos outros laboratórios. O endereçamento correto das máquinas é garantido através de um servidor DHCP que associa o MAC Address das máquinas de um determinado laboratório à sua respectiva rede. Computadores que não tem seu MAC Address associado a um endereço IP fixo utilizam o endereçamento 10.0.254.0/16 ao se conectarem a rede.

Também está disponível acesso Wi-Fi a partir de três pontos de acesso (Access Point – AP) denominados de labs-wifi (10.0.0.8) e labs-wifi-2 (10.0.0.9) e lab-wifi-5 (10.0.0.7). Utiliza como controle de acesso apenas uma senha WPA2 divulgada abertamente para os alunos e demais membros da comunidade acadêmica.

Em termos de equipamentos, todos os laboratórios fazem uso de switches de 48 portas e todos estes laboratórios estão ligados a um roteador/*firewall*. A figura 6 apresenta o diagrama da rede dos laboratórios.

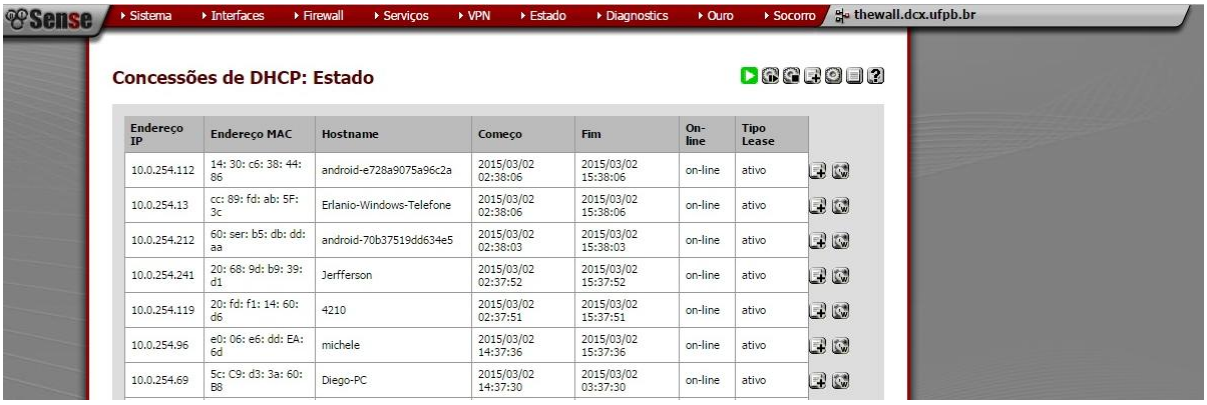


A infraestrutura física da rede dos laboratórios pode ser vista na figura 6.

4.2.2 Infra estrutura de Serviços

A infra estrutura de Serviços dos laboratórios é suportada por diversos softwares de rede para controle de acesso e autenticação, servidor de arquivos, DHCP, DNS, Proxy de rede, dentre os quais destacam-se como mais importantes no contexto deste trabalho o Squid, LightSquid, Samba, LDAP e PfSense.

O Pfsense é utilizado em todas as formas de acesso a rede dos laboratórios, tanto para quem utiliza a rede cabeada quando a rede Wi-FI, ele é um Firewall (controla tráfego de entrada e saída na rede), fornece via DHCP o endereçamento da rede de acordo com a seção anterior, implementa um Proxy de rede Squid para cache de tráfego web e também o serviço de resolução de nomes (DNS).

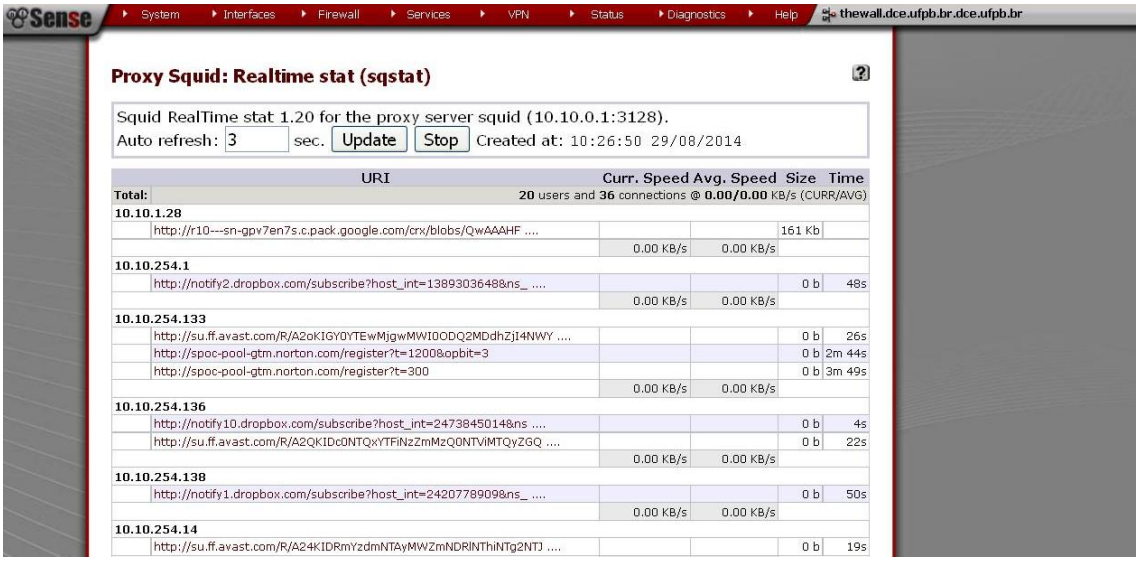


Endereço IP	Endereço MAC	Hostname	Começo	Fim	On-line	Tipo Lease
10.0.254.112	14: 30: c6: 38: 44: 86	android-e728a9075a96c2a	2015/03/02 02:38:06	2015/03/02 15:38:06	on-line	ativo
10.0.254.13	cc: 89: fd: ab: 5F: 3c	Erlanio-Windows-Telefone	2015/03/02 02:38:06	2015/03/02 15:38:06	on-line	ativo
10.0.254.212	60: ser: b5: db: dd: aa	android-70b37519dd634e5	2015/03/02 02:38:03	2015/03/02 15:38:03	on-line	ativo
10.0.254.241	20: 68: 9d: b9: 39: d1	Jerfferson	2015/03/02 02:37:52	2015/03/02 15:37:52	on-line	ativo
10.0.254.119	20: fd: f1: 14: 60: d6	4210	2015/03/02 02:37:51	2015/03/02 15:37:51	on-line	ativo
10.0.254.96	e0: 06: e6: dd: EA: 6d	michele	2015/03/02 14:37:36	2015/03/02 15:37:36	on-line	ativo
10.0.254.69	5c: C9: d3: 3a: 60: B8	Diego-PC	2015/03/02 14:37:30	2015/03/02 03:37:30	on-line	ativo

Figura 7 – Serviço de Resolução de Nome no PfSense

O sistema de *Registro* atualmente implementado nos laboratórios conta com o Squid, que é um proxy de aplicação que atua de maneira transparente nas conexões de aplicação Web, interceptando o tráfego dos usuários e realizando *cache* de informações. Essa atividade de conexão das aplicações e cache permanece registrada pelo Squid no PfSense, que utiliza uma aplicação adicional, chamada de LightSquid, para análisar e apresentar de maneira mais objetiva e clara estes registros.

A figura 8 mostra o Squid capturando os IP's que estão conectados a rede, neste exemplo ele tem um processo para atualizar-se a cada 3 segundos para identificar os IP's que estão ativos ou não.



URI	Curr. Speed	Avg. Speed	Size	Time
Total:	**20** users and **36** connections @ **0.00/0.00** KB/s (CURR/AVG)			
10.10.1.28				
http://r10---sn-gpv7en7s.c.pack.google.com/crx/blobs/QwAAAHF			161 Kb	
	0.00 KB/s	0.00 KB/s		
10.10.254.1				
http://notify2.dropbox.com/subscribe?host_int=1389303648&ns_			0 b	48s
	0.00 KB/s	0.00 KB/s		
10.10.254.133				
http://su.ff.avast.com/R/A2oKIGY0YTEwMjgwMWI0ODQ2MDdhZjI4NWY			0 b	26s
http://spoc-pool-gtm.norton.com/register?t=1200&opbit=3			0 b	2m 44s
http://spoc-pool-gtm.norton.com/register?t=300			0 b	3m 49s
	0.00 KB/s	0.00 KB/s		
10.10.254.136				
http://notify10.dropbox.com/subscribe?host_int=2473845014&ns			0 b	4s
http://su.ff.avast.com/R/A2QKIDc0NTQxYTFiNzZmMzQ0NTViMTQyZGQ			0 b	22s
	0.00 KB/s	0.00 KB/s		
10.10.254.138				
http://notify1.dropbox.com/subscribe?host_int=2420778909&ns_			0 b	50s
	0.00 KB/s	0.00 KB/s		
10.10.254.14				
http://su.ff.avast.com/R/A24KIDRmYzdmNTAyMWZmNDRlNThiNTg2NTJ			0 b	19s

Figura 8- Captura de IP pelo Squid

Além do PfSense e do Squid, também se faz uso do Light Squid nos laboratórios, ele é o analisador de registro do Squid. Com ele é possível gerar relatórios de acessos diários, assim é possível ver o IP que acessou a rede em determinada data e o intervalo de tempo do acesso, pois ele também mostra á horado acesso.

Nos laboratórios 1 e 2 se faz uso do sistema de autenticação via LDAP, que é utilizado para as máquinas com o sistema Linux onde se autentica no servidor central, que está localizado na "sala dos servidores" e apenas pessoas autorizadas tem acesso a esta sala. Para máquinas Windows nestes laboratórios não se tem o processo de autenticação, se utiliza o usuário padrão Aluno, e não tem base de dados centralizada.

Um sistema mais recente para autenticação é implementado para o Windows e Linux utilizando o Samba 4, emulando de maneira completa um Controlador de Domínio chamado de Active Directory, bastante comum para ambientes Windows com autenticação centralizada. Esta solução está implementada atualmente no Laboratório 5, em fase de teste e adaptações, e se mostra bastante adequada no contexto dos Laboratórios por criar um modelo de autenticação centralizada, tanto para o ambiente Linux e Windows, e assim fornecendo mecanismos de controle e centralização das atividades dos usuários dos laboratórios.

4.3. Cenários de Uso dos Laboratórios

A análise dos laboratórios permitiu levantar diversos pontos de controle que devem ser adequados de acordo com o que especifica o Marco Civil da Internet. Como já apresentado, esses controles devem ser feitos levando-se em conta a utilização da norma NBR, que vai guiar e especificar quais controles utilizar no levantamento realizado nos laboratórios.

4.3.1 Cenários

A abordagem da análise se deu através da formulação de cenários compatíveis com o uso diário dentro dos laboratórios em estudo. A partir desses cenários teremos uma análise considerando o ponto de vista do usuário – o que é possível fazer, como se autenticar e ter acesso a rede e do ponto de vista do administrador de sistema, identificando quais informações são armazenadas pelos serviços em execução que controlam autenticação, acesso aos computadores, acesso a Internet, entre outros.

Cenário 1: Acesso a partir dos computadores do laboratório 1 e 2.

Ao ter acesso a um computador do laboratório, o usuário tem a sua disposição dois sistemas operacionais para sua escolha: Linux e Windows. Do ponto de vista do Windows, temos acesso à opção de iniciar como Aluno ou Administrador.

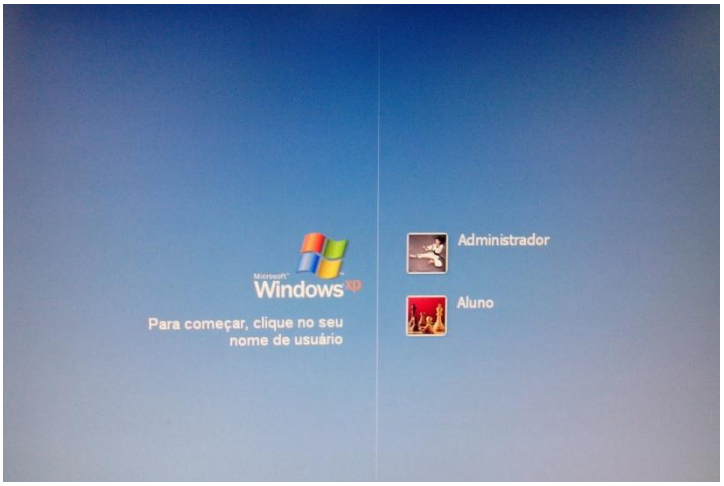


Figura 9- Tela de acesso ao sistema Windows (válido nos laboratórios 1 e 2)

Os alunos devem escolher a opção aluno para ter acesso a todas as funcionalidades do sistema, podendo ter acesso a rede sem maiores problemas. Se escolher a opção Administrador será pedido uma senha onde apenas os responsáveis pela manutenção dos laboratórios tem acesso as mesmas.

Com isso podemos observar que para uso do Windows no Laboratório, não se tem o processo de autenticação dos alunos, pois é utilizado o padrão de autenticação "aluno", também não se tem uma base de dados, com isso não existe registro de acesso para usuários Windows.

Como os laboratórios utilizam o firewall PfSense trabalhando junto ao Squid essa é a única forma de controle e monitoramento para os usuários deste sistema, pois vai ser possível ver o IP que esta ativo, seus sites acessados além da data e hora, mas não saberemos o aluno responsável pelo IP já que não é utilizado processo de autenticação.

Do ponto de vista Linux o aluno terá que passar por um processo de autenticação, fornecendo o nome do usuário e a senha para poder usar o sistema operacional e ter acesso a rede do laboratório.

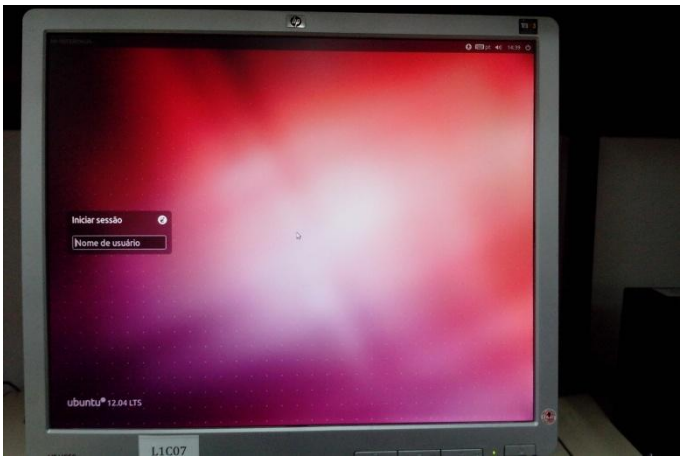


Figura 10 - Tela de Autenticação no Linux

Os laboratórios utilizam o PfSense junto com o Squid como foi visto na seção 1.1. Além disso as máquinas com Linux utilizam o sistema de autenticação via LDAP, onde ela se autentica no servidor central, que está localizado na "sala dos servidores" e apenas pessoas autorizadas tem acesso a esta sala. Os registros das máquinas Linux ficam no servidor, mas esta opção não esta configurada. O acesso aos registros (log) pode ser feito apenas pelos participantes do Projeto Tigers que ajuda na manutenção da rede e funcionamento dos laboratórios de informática, além do professor Carlos Dias que é responsável pelos laboratórios e por Bruno que é o analista de TI do CCAE. O acesso a estas informações é variável de acordo com o projeto envolvido e não se tem diferenciação de privilégios sobre as informações que podem ser obtidas e analisadas destes laboratórios.

Cenário 2 : Acesso a partir dos computadores do Laboratório 5

O Laboratório 5 foi recentemente aberto para o uso dos alunos e professores, ele conta com sistema de autenticação com um login composto por nome e senha para os dois sistemas operacionais presentes em suas máquinas (Linux e Windows). Conta com uma base de dados de usuários, e após o login tem acesso a todas as funcionalidades do sistemas. Por contar com a base de dados ele consegue identificar o usuário e seu registro de conexão. Mas não mantém guardados os registros de conexão sob sigilo e em ambiente controlado.

Cenário 3 : Acesso através dos computadores pessoais

Neste cenário analisaremos o uso de computadores pessoal, onde para se ter acesso é necessário que os usuários estejam ao alcance da rede Wi-Fi e saibam a senha de

autenticação. A partir do momento que os usuários tem acesso a esta senha, eles podem acessar a rede e navegar na Internet direto de seus computadores pessoais.

Para melhor compreensão destes cenários, mostraremos uma tabela resumo dos 3 cenários de uso dos laboratórios

		Lab 01 e 02	Lab 05	Computador Pessoal
Usuário	Processo de Autenticação	Parcial. Só os usuários Linux se autenticam.	Sim	Não. Autenticação padrão para uso da rede.
	Acesso as Funcionalidades do Sistema	Sim	Sim	Sim
Administrador	Registro de Aplicação	Através do PfSense	Através do PfSense	Através do PfSense
	Registro de Conexão	Parcial no Windows e Completo no Linux	Sim	Parcial. Identifica IP, data inicial e final de acesso, data. Mas não identifica usuário
	Guarda dos Registros de Conexão sob Sigilo e em Ambiente Controlado	Não	Não	Não

Tabela 2: Resumo dos Cenários de uso dos Laboratórios

Para um melhor entendimento dos Cenários de uso dos laboratórios, dividimos na tabela dois pontos de vista, o dos usuários e o dos administradores dos laboratórios e em seguida mostraremos a análise dos critérios selecionados.

O Processo de Autenticação é um critério definido e analisado, pois influencia na geração de registros de uso dos serviços do laboratório. Dependendo do que está implementado será possível individualizar um acesso ao sistema ou não. Por exemplo, de acordo com a tabela 1, o "Processo de Autenticação" não gera registro suficiente para identificar unicamente um usuário que acessa o sistema Windows em determinado momento, porém no Linux é possível obter essa informação.

O Acesso as Funcionalidades do Sistema indica o que está disponível para uso por parte dos usuários após o Processo de Autenticação, e essas funcionalidades do sistema pode variar da execução de programas computacionais, até o uso.

O Registro de Aplicação é onde fica armazenado as informações do que os usuários buscam ou postam na Internet e é proibido o armazenamento do Registro de Aplicação por parte dos provedores de conexão de acordo com o Marco Civil.

O Registro de Conexão é a possibilidade de identificarmos um usuário em nossa rede, identificando seu IP, data de acesso, e o horário que esse usuário interage on-line.

A Guarda dos Registros de Conexão sob Sigilo e em Ambiente Controlado é a forma com que deve ser armazenada os registros de conexão para que se preserve a privacidade dos usuários armazenando essas informações em ambientes onde só pessoas autorizadas tenham acesso a estes dados e que eles sejam preservados de maneira sigilosa.

5. ADEQUANDO AO MARCO CIVIL

O Marco Civil fala que: “a guarda e a disponibilização dos registros de conexão e de acesso a aplicação de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicação privadas, devem atender a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas”. (BRASIL,Lei n°2.126).

A NBR ISO diz que a organização deve estar acordo com todos os requisitos legais relevantes, aplicáveis para suas atividades de monitoramento. Assim para que os laboratórios analisados possam estar de acordo com o que é definido no Marco Civil da Internet, algumas medidas devem ser tomadas em relação ao uso da Internet nos nossos laboratórios, descritas nas seções a seguir.

Para entendermos melhor a situação dos nossos laboratório, veremos uma tabela especificando como esta a situação atual de cada laboratório, o que esta presente ou não para termos um melhor direcionamento na implantação do Marco Civil.

5.1 Registro de Conexão

A seguir teremos o que o Marco Civil fala sobre o registro de conexão, o que devemos ter sobre este registro e a NBR que fala o que devemos implantar para estes registros.

De acordo com o Marco Civil o “registro de conexão: o conjunto de	A NBR ISO 27002 fala que “O uso de procedimentos de monitoramento é

informações referentes a data e hora de inicio e término de uma conexão a Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;"(BRASIL,Lei n°2.126).	necessário para assegurar que os usuários estão executando somente as atividades que foram explicitamente autorizadas." Sobre os Registros (*log*) de administrador e operador a NBR ISO fala que as atividades dos administradores e operadores do sistema sejam registradas, com as seguintes diretrizes: a) a hora em que o evento ocorreu (sucesso ou falha); b) informações sobre o evento (exemplo: arquivos manuseados) ou falha (exemplo: erros ocorridos e ações corretivas adotadas); c) que conta e que administrador ou operador estava envolvido; d) que processos estavam envolvidos.

Tabela 3: Registro de Conexão de Acordo com o Marco Civil e a NBR 27002

Como vimos na seção 2.5 que trata das ferramentas utilizadas no laboratório e na 3.2.2 onde tratamos da infra estrutura de serviços, mostrando como as ferramentas dos laboratórios funcionam, podemos concluir que estamos parcialmente de acordo com o Marco Civil, pois podemos obter o endereço IP , a hora de acesso e a data de acesso dos usuários com ajuda das ferramentas que já fazemos uso em nossos laboratórios. Pois o PfSense filtra toda comunicação, transmitindo e recebendo dados. O Squid trabalha registrando todos os pedidos de conexão de aplicação web e fazendo cache dessas informações e com o uso do Light Squid podemos obter os relatórios de acesso diários dos usuários á Internet, estes relatórios contem o endereço IP, a data e o horário de acesso, com isso estamos de acordo com o registro de conexão do Marco Civil. Mas, para ficarmos de acordo com a NBR além do que pede o Marco Civil é preciso associar a "conta, e que administrador ou operador estava envolvido", para isso é necessário o uso de um processo de autenticação.

Atualmente, o processo de autenticação se faz presente para usuários Linux dos laboratórios 1 e 2, e para todos os usuários do laboratório 5 independente do sistema operacional, estes ,para terem acesso ao sistema precisam fornecer seu login e senha, a partir disso podem acessar, por exemplo, a Internet e, a partir daí o PfSense, junto ao Squid e Light Squid podem associar seu ID ao registro de conexão ..

Para resolver este problema de autenticação dos usuários Windows dos laboratórios 1 e 2, pode ser adotada a infra estrutura utilizada no laboratório 5, que utiliza os mesmos softwares dos laboratórios 1 e 2 (PfSense, Squid, Light Squid), mais o Samba 4 que é um sistema de autenticação implementado para o Windows e Linux, ele emula de maneira completa um Controlador de Domínio chamado de Active Directory, bastante comum para ambientes Windows com autenticação centralizada.

Com isso os usuários passarão a ter um processo de autenticação também no Windows, com isso ele passa a ter uma base de dados e ter seu registro de conexão informando o usuário, IP, data e horário de acesso, de acordo com o que diz as especificações do Marco Civil e da NBR 27002.

Outra solução de adequação dos laboratórios 1 e 2 é a introdução de um portal de autenticação, conhecido por Captive Portal, trabalhando junto com o Free Radius e que será abordada a seguir.

5.1.1 Autenticação com Captive Potal e Free Radius

O Captive Portal faz a captura de conexão pelo firewall e faz o redirecionamento para interface de gerenciamento de rede. Essa interface pode ser uma tela de aviso, um sistema de login, ou geração de Voucher para acessos temporários, com isso o usuário tentará fazer acesso pelo navegador e será direcionado para esta tela de autenticação (Hanai, Rafael Akira). O Captive Portal é um sistema de autenticação baseado no LDAP que já é utilizado em nestes laboratórios. Junto ao Captive Portal se faz necessário o uso adicional de um software chamado Free Radius, que é um servidor de autenticação que funciona atrelado ao Pfsense, pois ele serve para interligar e fazer o gerenciamento de autenticação junto ao banco de dados onde estão registrados os id’s dos usuários para realizar a autenticação junto ao Captive Portal. (Pereira, Marcos Heisy)

Apenas usuários cadastrados na base de dados poderão navegar. Alguns usuários de nossos laboratórios já possuem um cadastro, sendo este o mesmo que é utilizado para autenticar usuários nas máquinas Linux, ou seja, uma base de usuários LDAP, e ele deverá ser

utilizado para o acesso a rede. Para os usuários não cadastrados deve ser fornecido vouchers de acessos que serão utilizados para acessos temporários, direcionados a usuários que não irão utilizar rede dos laboratórios com frequência. Com isso, ao invés deles se autenticarem através do login existente em uma base de dados, o acesso se dará através de chaves de acessos destes vouchers que são gerados automaticamente pelo PfSense e contém um limite de tempo de conexão pré estabelecida. Quando os usuários não cadastrados ele forem acessar a rede será pedido o número da chave de acesso do voucher, assim teremos como identificar o usuário pela chave fornecida, pois para obter esse voucher o usuário terá que procurar com antecedência um dos responsáveis pelos laboratórios e se identificar, com isso será atrelado em um registro de conexão a identificação do usuário junto da chave do voucher. Esta solução também se torna adequada para a rede Wi-Fi pois ela também não identifica o usuário que está utilizando a rede e a partir desta implantação podeá identificar quem é o usuário da rede.

O Captive Portal é baseado no MAC Address, ele captura as informações (IP, MAC, USERNAME) antes de entregar o endereço de IP para o cliente através do firewall. Com isso podemos identificar qual o usuário que está utilizado nossa rede através de seu username, o IP e Mac utilizados por este usuário.

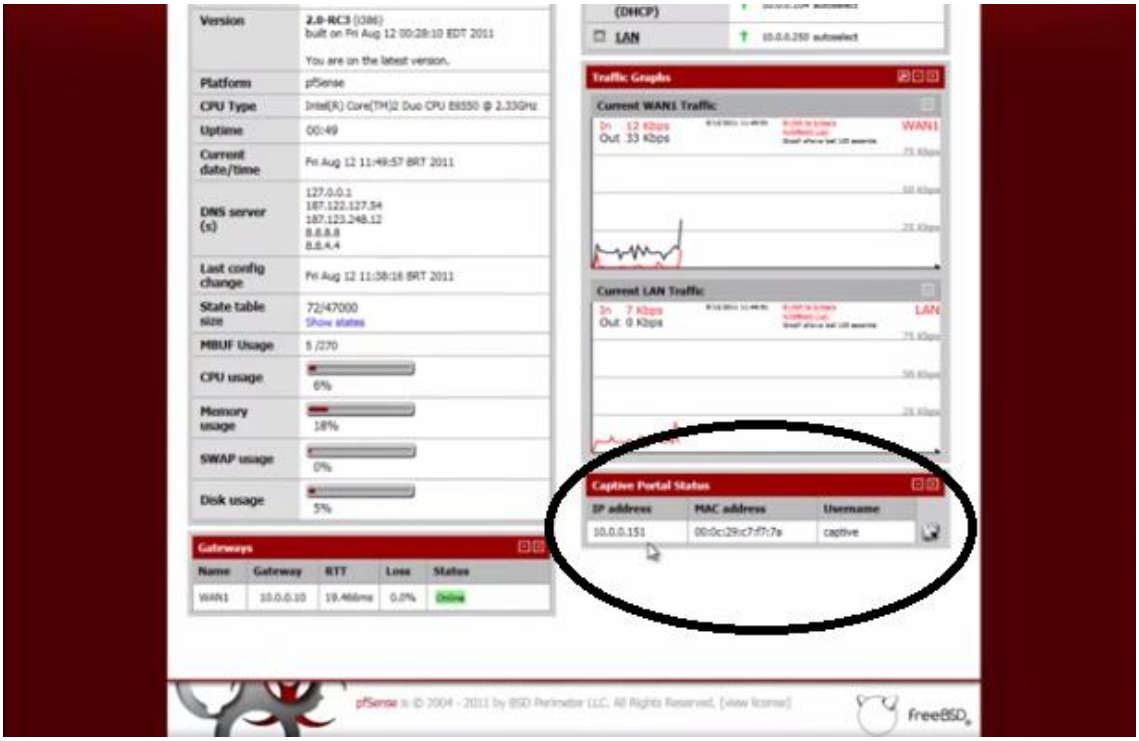


Figura 11 Tela Principal do PfSense, com o Captive Portal informando o IP, Mac e Username do Usuário logado

Um ponto a ser levado em consideração é sobre o Registro de Aplicação, o Marco Civil fala que é vedado ao provedor de conexão armazenar os Registros de Aplicação dos usuários, que são os sites que ele acessam ou o que eles postam em redes sociais. Com as ferramentas utilizadas nos laboratórios se pode ter acesso a estas informações, mas o Marco Civil só estará sendo descumprido se estas informações forem armazenadas, que no caso não ocorre.

5.2 Sigilo

Marco Civil	NBR 27002
De acordo com a Subseção I do projeto de lei, cujo titulo é Da Guarda de Registros de Conexão e diz que "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 um ano, nos termos do regulamento".	A NBR ISO fala que "Convém que registros *(log)* de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento de controle de acesso"

Tabela 4: Sigilo segundo o Marco Civil e a NBR 27002

A NBR ISO 27002 trata do sigilo da informação em uma subseção chamada Acordos de Confidencialidade onde ela fala que os requisitos para a confidencialidade ou acordos de não divulgação vai de acordo com a necessidade da organização para a proteção da informação. Para proteger essas informações confidenciais é necessário a utilização de meios legais e devem ser considerados alguns :

- Elementos como a classificação da informação a ser protegida (exemplo : informação confidencial),
- O tempo de duração do acordo de confidencialidade,
- As ações que devem ser tomadas quando o acordo esta encerrado,
- As ações e responsabilidades para evitar a divulgação não autorizada das informações,
- O uso permitido da informação,
- O direito de auditar e monitorar as atividades que envolvem as informações.

“Acordos de confidencialidade e de não divulgação protegem as informações da organização e informam aos signatários das suas responsabilidades, para proteger, usar e divulgar a informação de maneira responsável e autorizada.”

“Pode haver a necessidade de uma organização usar diferentes formas de acordos de confidencialidade ou de não divulgação, em diferentes circunstâncias.” (NBR ISO 27002)

O sigilo hoje em dia quanto as informações dos usuários se da devido ao comportamento ético de todos os funcionários que administram os laboratórios, pois falta uma política de uso da informação ou acordos de confidencialidade, estes acordos podem ser definido pelos responsáveis pelo funcionamento dos laboratórios e que vá de acordo com o que é proposto na instituição e no que diz o Marco Civil e que estes utilizem meios legais para isto. As informações devem passar a ser protegidas de acordo com sua definição, como por exemplo: (informação confidencial, informação restrita, etc.) e deve ser criada uma escala pra definir quais são as pessoas que podem ter acesso a cada tipo de informação (ex: Responsável pelos Laboratórios pode ver todos os tipos de informações mas os estudantes que participam do Tigers só podem ver as informações confidenciais) O tempo de duração do armazenamento desta informação deve ser de 1 ano, após este tempo o responsável pela administração da rede pode excluir estes arquivos, também deve ser determinantemente proibido a transferência de arquivos a partir desta sala e deve ser estabelecido níveis de acesso a informação que estão armazenadas nessa sala. Auditorias com essas informações só podem ser utilizadas se o usuário da rede ferir os bons costumes estabelecidos nas leis e com isso a Instituição correr risco de sair prejudicada.

5.3 Ambiente Controlado

O Marco Civil fala que: “a guarda e a disponibilização dos registros de conexão e de acesso a aplicação de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicação privadas, devem atender a preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas”.(BRASIL,Lei n°2.126).

Segundo a NBR ISO 27002 “Os registros (*log*) de auditoria podem conter dados pessoais confidenciais e de intrusos. Convém que medidas apropriadas de proteção de privacidade sejam tomadas (ver 15.1.4).” (NBR ISO)

Áreas de Segurança é o espaço físico que precisa ser protegido contra as ameaças que poderiam gerar um incidente de segurança da informação. Esse espaço considerado como área crítica tem importância e valor para organização, e necessita de proteção física:

- Difícil acesso para o público,
- Portas e janelas devem permanecer trancados,
- Equipamentos de detecção de intrusos devem ser instalados,
- Seja considerado equipamentos de combate a incêndios e desastres naturais.
- Essas áreas com acesso público deve ser controlado através da definição de um perímetro de segurança que aumenta o nível de segurança. (Campos, Sergio)

Já na sessão sobre as Áreas Seguras a Norma tem como objetivo é de prevenir o acesso físico não autorizado, danos ou interferências às instalações de uma organização. Com isto faz parte do contexto de áreas seguras o Perímetro de segurança física, Proteção contra ameaças externas e do meio ambiente e Trabalho em Áreas seguras. "A norma NBR ISO/IEC 27002 estabelece que um perímetro de segurança seja uma área física isolada que o acesso é controlado pelos seguintes controles de entrada física:

1. Porta com mecanismo de controle de acesso através de cartão ou uma área de recepção ou balcão com recepcionistas.

2. Uso de proteção como portas e janelas trancadas.

3. Sistemas adequados de detecção como alarmes.

O objetivo do perímetro de segurança é dificultar o acesso aos ativos através de uma dessas barreiras física. As áreas de segurança também podem ser implantados controles de acesso através de senhas que além da segurança, garante registro de todos os acessos que podem ser utilizados por eventuais auditorias. Deve-se levar em conta na definição do perímetro, a importância dos ativos para definir os investimentos em controles, além da sintonia dos colaboradores com uma cultura de segurança da informação. Esta cultura deve ser divulgada em toda empresa." (Campos, Sergio)

Já para o trabalho nas Áreas Seguras se faz necessária as seguintes diretrizes:

- O publico só terá conhecimento sobre a existência das áreas seguras ou das atividades realizada nelas realizadas se for necessário.
- Deve ser evitado o trabalho não supervisionado nestas áreas.
- As áreas que não estão sendo ocupadas fisicamente devem ser trancadas
- Não seja permitido o uso de maquinas fotográficas, gravadores de vídeo ou áudio ou de outros equipamentos de gravação, tais como câmeras em dispositivos móveis, salvo se for autorizado.

Para isto o registros de conexão devem ser armazenado em ambiente seguro, para isto a "Sala dos Servidores" onde deve ficar a base de dados com os registros de conexão dos usuários deve ser monitorada por câmera e com um sistema de detecção de presença (ex: alarmes). A sala não deve conter identificação externa para evitar que pessoas não autorizadas tentem obter acesso a mesma, e sempre que possível deve-se ter a presença de no mínimo um segurança nas imediações da sala. Apenas as pessoas autorizadas devem ter acesso a esta sala, como por exemplo, o Diretor do Centro, o Chefe do Departamento e os responsáveis pelo funcionamento da rede do laboratório. A sala deve ser refrigerada para evitar o superaquecimento dos servidores e conter extintores de incêndio em sua área interna e imediações. Todos os funcionários que terão acesso a sala devem estar devidamente identificados e deve haver o registro da hora de entrada e saída de cada pessoa na sala e de preferência que seja evitado trabalhos não supervisionados nessas áreas. A visita de terceiros a este ambiente só deve ocorrer junto da presença de algum responsável.

Se faz de grande necessidade a criação de uma política de controle de acesso para o uso da rede dos laboratórios de informática, essa política deve ser discutida entre os envolvidos no uso dos laboratórios, documentada e amplamente divulgada para que todos tenham conhecimento dos seus direitos e deveres em relação ao uso dos laboratórios. É conveniente que as regras de controle de acesso estejam claramente estabelecidas neste documento. Alguns requisitos para este documento:

- Política de disseminação e autorização da informação
- Responsabilidade de cada um dos envolvidos no uso dos laboratórios.
- Política de uso as rede
- Utilização de identificador de usuário (ID) único
- Assinatura de uma declaração para manter a confidencialidade da sua senha pessoal
- Solicitar a alteração das senhas que são fornecidas temporariamente.

Além de alguns aspectos relacionados a responsabilidade dos usuários quando ao uso de senhas

- Manter a confidencialidade
- Alterar a senha com frequência
- Criar senhas de qualidade
- Modificar a senha regularmente
- Não compartilhar suas senhas

6 CONCLUSÃO

Este trabalho abordou a análise dos laboratórios de informática dos cursos de Sistemas de Informação de maneira a adequá-los a recente lei chamada de Marco Civil da Internet no que descreve os direitos e deveres dos usuários de Internet no Brasil e que tem como foco principal neste trabalho a Guarda dos Registros de Conexão sob Sigilo e em Ambiente Controlado, tendo com guia de implantação para estas adequações a NBR 27002.

O trabalho fez uma análise do textos do Marco Civil e da seção da 10.10 da NBR 27002 chegando a uma correlação entre os pontos abordados neste trabalho sobre os registros de conexão.

A partir da convergência, na análise dos laboratórios levantou-se toda a infra estrutura existente nos laboratórios e alguns cenários de uso dos mesmos e o que está implementado para auxiliar na administração do uso de sua rede.

De posse da análise, pode-se verificar que estes laboratórios já se contam com algum certo grau de adequação precisando apenas de alguns ajustes para ficar de acordo com o que é pedido no Marco Civil. O registro de Conexão já se encontra em funcionamento de maneira correta no laboratório 5 e parcialmente nos Laboratórios 1 e 2, precisando de ajuste apenas para os usuários Windows e para os que utilizam a rede Wi FI .

Por fim, verificamos que não existia forma de guardar os registros de conexão de maneira sigilosa e em ambiente controlado. Para isso, usamos a NBR 27002 que da as diretrizes de como se implantar um Ambiente Controlado e o Sigilo das informações. A partir

das propostas feitas, os laboratórios ficam de acordo com o que é pedido no Marco Civil no que diz respeito a guarda do Registro de Conexão, sob Sigilo e em Ambiente Controlado.

6.1 Limitações e Trabalhos Futuros

Por o Marco Civil ser um tema bastante recente foi muito difícil encontrar fontes de pesquisa sobre ele, poucas fontes mostravam um conteúdo abrangente que pudesse atender a necessidade deste trabalho, por conta disso, na maioria das vezes foi necessário recorrer a matérias de jornais ou revistas especializadas.

Nas visitas aos laboratórios todas as observações foram possíveis e sem empecilhos, como também o acesso ao funcionamento das ferramentas de controle da rede presentes nos laboratórios.

Para trabalhos futuros é proposto um estudo sobre o funcionamento da rede Wi-Fi dos Laboratórios do Curso de Sistemas de Informação do Campus IV da UFPB e sobre processos de autenticação para redes Wi-Fi para estes ficarem de acordo com o Marco Civil da Internet

REFERÊNCIAS BIBLIOGRÁFICAS

Associação Brasileira de Normas Técnicas-ABNT. Tecnologia da Informação-Técnicas de Segurança- Código de Prática para a gestão da Segurança da Informação- NBR ISO 27002. 2 ed. 2005.

Anderson, Kevin**. Hackers atacam site da Casa Branca**. Disponível em < http://www.bbc.co.uk/portuguese/noticias/2001/010505_hackers.shtml > Data de Acesso 13/07/2014

Aras, Vladimir. **Breves comentários ao Marco Civil da Internet**. Disponível em <http://blogdovladimir.wordpress.com/2014/05/05/breves-comentarios-ao-marco-civil-da-internet/ > Data de Acesso: 16/05/2014

BRASIL. **Subemenda Substitutiva Global ás Emenda de Plenário ao Projeto de Lei N°2.126**, de 2011. Brasília 2014

Cartilha de Segurança para a Internet. Disponível em <http://cartilha.cert.br/mecanismos/ > Data de Acesso 17/07/2014

CHESWICK, William R. **Firewalls e Segurança na Internet. Repelindo o Hacker Ardiloso2**.ed. Porto Alegre: Bookman, 2005

COBIT Security Baseline / IT Governance Institute, 2ª edição. 2007.Disponível em < http://www.itgovernance.co.uk/products/885>. Data de acesso: 03/06/2014.

Furutani, Roberto. **Autenticação e obtenção de dados via LDAP**. Disponivel em <http://www.furutani.com.br/2008/09/autenticacao-e-obtencao-de-dados-via-ldap/> Data de Acesso 10/07/2014

G1,Globo.**Entenda o caso de Edward Snowden, que revelou espionagem dos EUA** Disponível em <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html> Data de Acesso 13/07/2014

Hanai, Rafael Akira. Rede Local Sem Fio e Captive Portal Como Meio de Interação Entre Restaurante e Cliente. Marília, SP:[s,n], 2014

Junior. A. E . A , Santos. Ernani Marques .**Controles e Práticas de Segurança da Informação em um Instituto de Pesquisa Federal**. SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA (2011).

KUROSE, James F.; ROSS, Keith W. Redes de Computadores e a Internet. 3ª Ed. São Paulo: Pearson, 2006.

LAGE, ALÉXIA. **Conhecendo a ABNT NBR ISO/IEC 27001**.Disponível em <http://www.profissionaisti.com.br/author/alagef/> Data de acesso 25/05/2014

Laureano, M.A. Pchek. **Instalando e Configurando o Squid**. Disponível em < http://www.mlaureano.org/guias_tutoriais/GuiaInstSquid.htm > Data de Acesso 17/07/2014

Leão, Felipe, **"Controle de Acesso a Dados em Sistemas de Informação através de Mecanismos de Propagação de Identidade e Execução de Regras de Autorização**." Simpósio Brasileiro de Sistemas de Informação (2011)

LOPO. Joana. **Legislação da Internet é considera Marco Histórico para Especialistas**. Revista TI Nordeste,Salvador,Nº15,p.23-<WBR>29,2014

MARCIANO, J. L. P. **Segurança da Informação – Uma Abordagem Social**. Brasília, 2006. 211f. Tese (Doutorado em Ciência da Informação) – Universidade de Brasília, Brasília, 2006.

Molon, Alessandro**. Entenda o Marco Civil**. Disponível em <http://www.molon1313.com.br/entenda-o-marco-civil-da-internet/> Data de acesso: 16/05/2014.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lucio. **Segurança de Redes em Ambientes Cooporativos**. São Paulo: Novatec, 2007.

Peixoto, Mario .**Segurança da informação: vale muito aplicar a ISO 27002** – Disponível em< http://webinsider.com.br/2012/11/12/seguranca-da-informacao-vale-muito-aplicar-a-iso-27002/ >

Pereira, Leonardo. **5 pontos essenciais para entender o Marco Civil da Internet** Disponível em <http://olhardigital.uol.com.br/noticia/41053/41053> Data de Aceso 16/05/2014

Pereira, Marcos Heyse. Segurança de Redes sem Fio, uma Proposta com Serviços Integrados de Autenticação LDAP e Radius. Pontifícia Universidade Católica do Paraná. Curitiba.Novembro,2009.

Rabaneda, Fabiano. **Os logs de acesso e sua guarda pelos provedores**. Disponível em < ttp://www.nic.br/imprensa/clipping/2010/midia165.htm > Data de acesso: 18/06/2014

RIBEIRO, Uirá; Certificação Linux. Rio de Janeiro: Ed. Axcel Books,2004. p. 181, p. 295-297.

Silva,P.T; Botelho,Hugo; Torres, C.B. Segurança dos Sistemas de Informação, **Gestão Estratégica da Segurança Empresarial**.Centro Atlantico pt,1ª edição, Portugal 2013. Pag 64-67http://www.semola.com.br/conceitos.html Acesso em 09/07/2014

TANEMBAUM, Andrew. **Sistemas Operacionais Modernos**. 2ª Ed. São Paulo: Pearson Prentice Hall, 2003.

Terra. **Marco Civil da Internet: O que muda na sua vida.** Disponível em <http://tecnologia.terra.com.br/marco-civil/> 26/05/2014