UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

UM MODELO DE GESTÃO PARA PREVENÇÃO DA MÁ UTILIZAÇÃO DA WEB

DISSERTAÇÃO DE MESTRADO

Ricardo Tombesi Macedo

Santa Maria, RS, Brasil

2012

UM MODELO DE GESTÃO PARA PREVENÇÃO DA MÁ UTILIZAÇÃO DA WEB

por

Ricardo Tombesi Macedo

Dissertação apresentada ao Programa de Pós-Graduação em Engenharia da Produção da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para a obtenção do grau de

Mestre em Engenharia da Produção

Orientador: Prof. Dr. Raul Ceretta Nunes (UFSM)

Santa Maria, RS, Brasil

2012

Cutter Tombesi Macedo, Ricardo

Um Modelo de Gestão para Prevenção da Má Utilização da Web / por Ricardo Tombesi Macedo. – 2012.
124 p.: il.; 31 cm.

Orientador: Raul Ceretta Nunes (UFSM)
Dissertação (Mestrado) - Universidade Federal de Santa Maria, Centro de Tecnologia, Programa de Pós-Graduação em Engenharia da Produção, RS, 2012.

1. Engenharia da Produção 2. Gerência 3. Má Utilização da *Web* 4. Prevenção 5. Políticas de Utilização da Internet 6. Políticas de Controle de Acesso Sensíveis à Atributos Contextuais 7. Aprimoramento Contínuo I. Ceretta Nunes (UFSM), Raul. II. Título.

CDU CDU

Ficha catalográfica elaborada por
Bibliotecatório que fez a CIP
Biblioteca Central da UFSM

E-mail: rmacedo@inf.ufsm.br

Universidade Federal de Santa Maria
Centro de Tecnologia
Programa de Pós-Graduação em Engenharia de Produção

A Comissão Examinadora, abaixo assinada,
aprova a Dissertação de Mestrado

UM MODELO DE GESTÃO PARA PREVENÇÃO DA MÁ UTILIZAÇÃO DA WEB

elaborada por
Ricardo Tombesi Macedo

como requisito parcial para obtenção do grau de
Mestre em Engenharia da Produção

COMISSÃO EXAMINADORA:

Raul Ceretta Nunes (UFSM), Dr.
(Presidente/Orientador)

Roseclea Duarte Medina, Profª. Drª. (UFSM)

Altair Olivio Santin, Prof. Dr. (PUC/PR)

Santa Maria, 05 de Março de 2012.

DEDICATÓRIA

Dedico essa conquista a todas as pessoas que me ajudaram, incentivaram e/ou torceram por mim.

AGRADECIMENTOS

Agradeço primeiramente a Deus pelas oportunidades proporcionadas e que tornaram possível adquirir o título de mestre.

Aos meus pais que sempre se esforçaram para me ensinar muito além de sua capacidade, sempre reforçando o valor dos estudos na vida das pessoas.

Ao professor Raul Ceretta Nunes por toda dedicação, paciência e por sempre procurar a melhor forma de me incentivar a desempenhar um bom trabalho.

Ao meu amigo Júnior Marcos Bandeira que me incentivou a entrar no mestrado. Ao meu amigo e colega de projeto Marcelo Colomé pela dedicação que teve em solucionar os problemas técnicos encontrados durante a pesquisa.

Aos colegas de laboratório, Bruno Mozzaquatro, Victor Alves e Renato Preigschadt Azevedo que sempre estiveram prontos a ajudar em toda dificuldade que encontrei e para discutir a melhor solução a ser empregada do ponto de vista científico.

A CAPES pelo fomento a pesquisa, fundamental para o desenvolvimento dos trabalhos.

A todas as pessoas não citadas que de forma direta ou indireta cooperaram para essa vitória, seja com conselhos, incentivos ou simplesmente por torcer pelo meu sucesso.

“No suporte, os comportamentos dos indivíduos têm sua explicação muito mais na espécie a que pertencem os indivíduos do que neles mesmos.
Falta-lhes liberdade de opção.
Por isso, não se fala em ética entre os elefantes.”
— PAULO FREIRE

RESUMO

Dissertação de Mestrado
Programa de Pós-Graduação em Engenharia de Produção
Universidade Federal de Santa Maria

UM MODELO DE GESTÃO PARA PREVENÇÃO DA MÁ UTILIZAÇÃO DA WEB

AUTOR: RICARDO TOMBESI MACEDO
ORIENTADOR: RAUL CERETTA NUNES (UFSM)

Local da Defesa e Data: Santa Maria, 05 de Março de 2012.

Atualmente, a utilização da *Web* no ambiente de trabalho tem proporcionado novos modelos de negócio, redução de custo com comunicação e agilidade nos processos empresariais. No entanto, a adoção desse recurso por parte das empresas não trouxe apenas benefícios, uma vez que se estima que 30 a 40% dos empregados utilizam de forma indevida essa tecnologia. Dentre as atividades indevidas mais praticadas encontram-se as compras *on-line*, jogos de *poker* e acessos a sites de pornografia. Tal comportamento, além de expor a rede da organização à vírus, gera um prejuízo estimado em 54 bilhões de dólares anualmente em perdas de produtividade. Observa-se na literatura, que a abordagem preventiva mais utilizada para tratar este problema consiste no emprego de Políticas de Utilização da Internet (PUI). Tal estratégia trata-se da especificação de diretrizes por parte dos empregadores determinando como a Internet deve ser utilizada no ambiente de trabalho. Apesar de sua larga utilização, o emprego de PUI apresenta dificuldades em relação ao cumprimento das diretrizes especificadas. Para contornar as dificuldades, pesquisadores tem aplicado tais diretrizes diretamente em filtros de acesso à Internet, através de Políticas de Controle de Acesso (PCA). Ao aplicar PCAs, a granularidade é um fator determinante para potencializar a utilização da *Web*. Visto que, considerando níveis extremos, tanto permissividade quanto restritividade ocasionam a má utilização da *Web*. Neste contexto é relevante explorar PCAs baseadas em listas, perfis e atributos contextuais, sendo que as baseadas em atributos contextuais apresentaram granularidade mais fina. Entretanto, na mesma proporção que se afina a granularidade, aumenta-se o custo no processo de elaboração das políticas. Além disto, a alta dinamicidade na disponibilização de recursos na *Web*, com o passar do tempo, pode tornar obsoletas as PCAs, mesmo se especificadas com granularidade fina, possibilitando novamente a utilização indevida da *Web*. Devido a esses fatores, incrementa-se a complexidade em conceber uma medida preventiva baseada em PCAs. Todavia, agregando os aspectos eficazes das PUIs, esta dissertação propõe um Modelo de Gestão para Prevenção da Má Utilização da Web que utiliza PCAs sensíveis à atributos contextuais. Tal modelo objetiva evitar que as PCAs tornem-se obsoletas ao aplicar um gerenciamento contínuo dessas políticas. Além disso, busca-se reduzir o ônus da elaboração e gestão das PCAs ao propor um *software* para transpor as necessidades dos gestores para PCAs sensíveis ao contexto, de modo que administradores sem conhecimentos técnicos específicos gerenciem de forma contínua PCAs baseadas em atributos contextuais. Um estudo de caso em uma instituição pública, cuja atividade fim trata-se do ensino superior, comprovou a aplicabilidade do modelo no ambiente de produção. Obteve-se como resultado a potencialização dos acessos à rede *Wireless* dessa instituição.

Palavras-chave: Modelo de Gestão, Controle de Acesso, Informações Contextuais, Má Utilização da Internet, Produtividade Empresarial.

ABSTRACT

Master's Dissertation
Graduate Program in Production Engineering
Federal University of Santa Maria

A MANAGEMENT MODEL FOR PREVENTS THE INTERNET BAD USAGE

AUTHOR: RICARDO TOMBESI MACEDO
ADVISOR: RAUL CERETTA NUNES (UFSM)
Defense Place and Date: Santa Maria, March 05th, 2012.

Currently, the use of the Web in the workplace has provided new business models, reduced communication cost and agility in business processes. However, some side effects also arise, since it is estimated that 30-40% of employees taken improperly use of this technology. Among the improper activities are online shopping, games playing and access to pornography sites. Besides exposing the organization's network to computer virus, such behavior causes around of 54 billion dollars annually in lost productivity. From literature, we know the most widely used preventive approach to address this problem is the use of Internet Use Policies (PUI), that corresponds to specification guidelines for employers in determining how the Internet should be used in the workplace. Despite its widespread use, the application of PUI presents difficulties in relation to compliance with the specified guidelines and these guidelines have been applied directly on Internet access filters through Access Control Policies (PCA). By applying PCA, the granularity is a key factor to ensure the web use control, claiming by contextual attributes manipulation that offer fine granularity. However, fine granularity increases the cost of PCA management, mainly because the dynamic changing of web user needs. This work proposes a management model for prevents Internet bad usage in the workplace by using context-based PCAs combined to a police continuous management framework to prevent the PCAs become obsolete. To facilitate the translation of needs to PCAs a software were developed to allow administrators without specific technical knowledge to continuous manage fine-grained PCAs. A case study has developed to validate the applicability of the model in a production environment. The result was the enhancement of a wireless network usage in an educational public institution.

Keywords: Management Model, Access Control, Contextual Information, Internet Bad Usage, Workplace Productivity.

LISTA DE FIGURAS

LISTA DE CÓDIGOS FONTES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABAC	*Atributed-Based Access Control*
CABEC	Controle de Acesso Baseado em Expressões Contextuais
DAC	*Discretionary Access Control*
DPCE	Direito de Privacidade nas Comunicações Eletrônicas
FTP	*File Transfer Protocol*
GSI	Gestão da Segurança da Informação
HTML	*Hypertext Markup Language*
HTTP	*Hypertext Transfer Protocol*
LDAP	*Lightweight Directory Access Protocol*
NWRC	*Non-Work-Related Computer*
MB	*Mega Bytes*
P2P	*Pear to Pear*
PCA	Políticas de Controle de Acesso
PDCA	*Plan-Do-Check-Act*
PERT	*Program Evaluation and Review Technique*
PHP	*Personal Home Page*: *Hypertext Preprocessor*
PUI	Políticas de Utilização da Internet
RADIUS	*Remote Authentication Dial In User Service*
RBAC	*Role-Based Access Control*
RUP	*Rational Unified Process*
SGBD	Sistema Gerenciador de Base de Dados
RUP	*Rational Unified Process*
TPB	*Theory of Planned Behavior*
TIB	*Theory of Interpersonal Behavior*
URL	*Uniform Resource Locator*
XACML	*eXtensible Access Control Markup Language*

SUMÁRIO

1 INTRODUÇÃO

O uso da Internet na atualidade é visto como posicionamento empresarial estratégico. Pois, além da redução de custos (HELPER; SAKO, 2010), a rede mundial de computadores proporciona novos modelos de trabalho (TAN et al., 2010). Pode-se associar a redução de custos à economia na comunicação e transporte devido à utilização de ferramentas que proporcionam mensagens instantâneas, teleconferências e acesso remoto. De maneira similar, podem-se associar os novos modelos de trabalho ao alcance de novos mercados geográficos e a novas modalidades de venda, tais como o *E-Commerce*, onde transações comerciais são realizadas através de equipamentos eletrônicos.

Entretanto, a *International Data Corporation*, empresa especializada em inteligência de mercado, estimou que 30 a 40% dos empregados com acesso à *Web* não a utilizam para desempenhar apenas atividades relacionadas com suas funções na empresa (LI; ZHANG; SARATHY, 2010). Em conseqüência disso, estima-se que a má utilização da Internet por parte dos funcionários custa 54 bilhões de dólares anualmente em perdas de produtividade (YOUNG, 2010). Dentre as atividades caracterizadas como má utilização da Internet durante o expediente de trabalho cabe destacar as compras *on-line*, jogos de *poker* e acesso a sites de pornografia (ARNESEN; WEIS, 2007). Além do prejuízo mencionado, tais atividades expõem a rede da organização a vírus e *spywares* (LIAO; LUO; LI, 2009).

Na literatura, encontram-se diversas abordagens para o problema da baixa produtividade empresarial em conseqüência da utilização indevida da *Web*. Apesar de não existir um senso comum quanto à classificação formal dessas abordagens, Chou, Sinha e Zhao (2010a) resumem os estudos recentes sobre o comportamento abusivo na Internet em três categorias: *Prevenção*, *Identificação* e *Monitoramento*. Na categoria de prevenção procura-se empregar medidas para impedir o acontecimento do comportamento abusivo (ANANDARAJAN, 2002). Na categoria de identificação visa-se diagnosticar fatores que induzem ao comportamento abusivo na Internet (GALLETTA; POLAK, 2003). Já na categoria de monitoramento estudam-se questões legais referente à aplicação de técnicas de acompanhamento das atividades dos funcionários na Internet (PANKO; BEH, 2002), de modo que, considerando a perspectiva dos direitos humanos, esta prática não interfira na privacidade desses indivíduos.

Considerando essa classificação, a estratégia mais empregada encontra-se na abordagem preventiva através da aplicação de Políticas de Utilização da Internet (PUI) (YOUNG, 2010).

Tais políticas expressam diretrizes estabelecidas pelos empregadores referentes ao uso dos recursos computacionais no local de trabalho (SIAU; NAH; TENG, 2002). A eficácia do emprego de PUI está relacionada com a conscientização dos empregados referente aos direitos dos empregadores e seus deveres (ARNESEN; WEIS, 2007). Entretanto, tal estratégia apresenta dificuldades quanto ao controle e ao cumprimento das diretrizes (CHOU; SINHA; ZHAO, 2010a).

Para contornar essa dificuldade, Rao e Jaeger (2009) aplicam Políticas de Controle de Acesso (PCA) diretamente em filtros de acesso à Internet. Ao empregar a abordagem baseada em PCA, a granularidade das políticas é um fator essencial para proporcionar aos gerentes a flexibilidade para controlar o acesso à *Web*, mas sem comprometer o potencial da utilização desse recurso no ambiente de trabalho (WILSON, 2009).

Em PCAs as listas de controle de acesso (SAMARATI; VIMERCATI, 2001) representam a forma mais primitiva de controle de acesso, permitindo uma granularidade grossa apenas. Políticas baseadas em perfis (FERRAIOLO et al., 2001) proporcionam facilidade no processo de gerenciamento. Entretanto, assim como as listas de controle de acesso sua granularidade é grossa. Já as PCAs sensíveis à atributos contextuais (YUAN; TONG, 2005) apresentam granularidade fina (MACEDO; NUNES; BANDEIRA, 2010), apesar da alta complexidade na especificação e manutenção (PRIEBE; DOBMEIER; KAMPRATH, 2006).

Além do desafio presente no processo de elaboração, nota-se que a alta dinamicidade na disponibilização de recursos na *Web* com o passar do tempo pode tornar obsoletas as PCAs, mesmo especificadas com granularidade fina. Devido a esse fato, pode-se possibilitar a utilização indevida da *Web*, causando novamente impactos negativos na produtividade dos funcionários. Em decorrência desses fatores, a complexidade para realizar um gerenciamento preventivo baseado em PCAs é aumentado.

Esta dissertação propõe um Modelo de Gestão para Prevenção da Má Utilização da *Web* que provê a criação e gerenciamento de PCAs através de um ciclo de melhoramento contínuo, relacionando PUIs com as ferramentas gerenciais: ciclo *Plan-Do-Check-Act* (PDCA) (NING; CHEN; LIU, 2010), Organogramas (DALE, 1955), *Brainstorming* (KOLFSCHOTEN, 2011), Diagramas *Program Evaluation and Review Technique* (PERT) (DOUGLAS, 1978) e Plano de Ação 5W2H (CESAR et al., 2005). Além disso, propõe-se um *software* para minimizar o processo de elaboração e manutenção de PCAs, possibilitando que gestores sem conhecimento técnico em uma linguagem de programação de PCA específica realizem o gerenciamento de PCA baseadas em atributos contextuais.

1.1 Motivação

Atualmente, ferramentas de telecomunicações tais como e-mail, mensagens instantâneas e o próprio acesso à Internet têm revolucionado a forma que as organizações gerenciam e controlam suas operações diariamente (LIAO; LUO; LI, 2009). No entanto, apesar dos benefícios gerados pela incorporação da Internet, estima-se que em média mais de 81 minutos das horas trabalhadas em um dia por um empregado, são desperdiçadas em atividades não relacionadas ao trabalho através dessa tecnologia (KLEIN, 2007). A prática de atividades abusivas por parte dos funcionários pode ocasionar vários problemas para as empresas, cabendo destacar:

- Perdas financeiras: estima-se um prejuízo de 54 bilhões de dólares anualmente para as empresas em decorrência da baixa produtividade causada pela navegação em sites da *Web* não relacionados com as atividades do trabalho (YOUNG; CASE, 2004);

- Possibilidade de denegrir a imagem da empresa: quando tornado público, casos como assédio sexual, racismo ou pedofilia no ambiente de trabalho através da Internet, podem denegrir/comprometer a imagem da organização perante a sociedade, causando impactos negativos nos negócios (YOUNG, 2010);

- Fácil aderência a distrações: 30 a 40% dos empregados com acesso à *Web* a utilizam em atividades não relacionadas ao trabalho (LI; ZHANG; SARATHY, 2010);

- Exposição a Vulnerabilidades: o acesso a determinados sites expõem a rede da empresa a vírus e *spywares* (GRIFFITHS, 2010);

1.2 Problema de Pesquisa

Na literatura encontra-se várias nomenclaturas para caracterizar a utilização indevida da *Web* no ambiente de trabalho, dentre elas: abuso da Internet (YOUNG; CASE, 2004), uso pessoal da *Web* (RAMAYAH, 2010), o trabalho computacional não relacionado (BOCK; HO, 2009), *Cyberslacking* (VITAK; CROUSE; LAROSE, 2011), *Cyberloafing* (RESTUBOG et al., 2011) e *Junk Computing* (CHEN; CHEN; YANG, 2008). Apesar de variadas, todas se referem à prática de atividades abusivas na Internet por parte dos funcionários, gerando perda de produtividade para as empresas ou empregadores. Este trabalho optou pela utilização do termo *má utilização da Web no ambiente de trabalho* (LIAO; LUO; LI, 2009), por melhor caracterizar essa ameaça em nosso idioma.

1.3 Objetivo Geral

Prover um Modelo de Gestão para Prevenção da Má Utilização da *Web*, que associe aspectos eficazes do emprego de PUIs ao gerenciamento contínuo das PCAs sensíveis à atributos contextuais. Ainda, propor um *software* que miniminize o ônus referente ao processo de elaboração e manutenção de PCAs, de modo que gestores sem conhecimento técnico em uma linguagem de programação de PCA específica, consigam realizar o gerenciamento contínuo.

1.4 Contribuições

Tem-se como principais contribuições:

- Apresentar um referencial teórico sobre a má utilização da *Web*.
- Argumentar sobre como o uso de PCAs com granularidade mais fina pode prover um acesso mais qualificado à *Web*.
- Propor um Modelo de Gestão para Prevenção da Má Utilização da Web.
- Propor um *software* para auxiliar a elaboração e manutenção de PCAs, minimizando o ônus deste processo.
- Realizar um estudo de caso envolvendo o modelo e *software* propostos.

1.5 Metodologia

A pesquisa apresentada classifica-se como quantitativa, devido as particularidades subjetivas, conforme a definição de Silva (2001). Quanto aos procedimentos técnicos utilizou-se o levantamento bibliográfico sobre o problema de pesquisa e o estudo de caso em uma instituição de ensino superior. Para mensurar a aplicabilidade do modelo e *software* proposto, utilizou-se o monitoramento de tráfego *Web* e aplicação de questionários semi-estruturados.

Do ponto de vista exploratório, considerou-se como premissa que no meio empresarial os funcionários desempenham suas atividades quase que exclusivamente em seu horário de expediente. Desse modo, considerando o problema de pesquisa, torna-se interessante pensar em medidas que otimizem o tempo gasto na Internet. Pois, ao evitar atividades não relacionadas ao trabalho, estes indivíduos desempenharão suas tarefas com maior eficiência e consequentemente apresentarão maior produtividade.

Considerando essa premissa em conjunto com o problema de pesquisa, assume-se que a granularidade das PCAs é um fator determinante para o sucesso do seu emprego como medida preventiva. Como hipótese, considera-se que se os líderes de equipes possuírem ferramentas administrativas que permitam realizar a elaboração e manutenção de PCAs com granularidade fina, se torna possível gerenciar o tempo gasto pelos funcionários na Internet, potencializando sua produtividade, dessa forma, a utilização de atributos contextuais nas PCAs podem aumentar a qualidade das regras de acesso.

Porém, devido a dinamicidade na disponibilização de recursos na rede mundial de computadores, tais PCAs devem ser atualizadas de forma contínua, reforçando um modelo de gestão que agregue aspectos eficazes das PUI em conjunto com uma ferramenta capaz de minimizar o ônus da elaboração e manutenção de PCAs.

Para auxiliar a validação do trabalho, foi desenvolvido um protótipo de *software* para interceptar as requisições de acesso para *Web*. O protótipo tem a responsabilidade de capturar o contexto em que o usuário se encontra, considerando o horário de acesso e as atividades delegadas à ele naquele dado momento. Caso os sujeitos estejam no período de alguma atividade, o protótipo avalia se as regras definidas por seu supervisor ou responsável permitem ou não o acesso ao recurso da *Web* requisitado.

Para executar o protótipo escolheu-se o ambiente acadêmico, pois o mesmo trata-se de um ambiente dinâmico, onde cada indivíduo pode ativar diversos papéis em função do tempo, e a cada papel ativado estar subordinado a níveis distintos de hierarquia. Como por exemplo, um aluno de mestrado pode ser em um determinado momento monitor de uma disciplina e em outro instante bolsista de um projeto de pesquisa e ainda enquanto exerce esses papéis estar subordinado a supervisores diferentes com opiniões discrepantes quanto a utilização produtiva da *Web*. Pode-se citar também o caso de funcionários que em determinados intervalos de tempo assumem posições variadas dentro da instituição como um cargo administrativo, acadêmico e até mesmo de aluno e também possuem uma hierarquia dinâmica de supervisores. Com estas características, o ambiente acadêmico apresenta diversas variações, apresentando complexidade significativa no gerenciamento de acesso à *Web*.

1.6 Organização da Dissertação

A dissertação está organizada como segue. O capítulo 2 expõe o problema de pesquisa da má utilização da Internet, citando o emprego das PUIs como estratégia mais utilizada em

medidas preventivas.

No capítulo 3, estudam-se as PCAs baseadas em listas, papéis e em atributos contextuais. Além disso referencia-se que na mesma medida em que se aumentam os atributos contextuais, aumenta-se a onerosidade no processo de gestão. O que torna um desafio o emprego dessa abordagem no problema de pesquisa em questão.

No capítulo 4 propõe-se o Modelo de Gestão para Prevenção da Má Utilização da Web, cujo objetivo é prover um processo de gerenciamento de PCAs com granularidade fina de forma contínua.

No capítulo 5 propõe-se o *software* para gerenciamento das PCAs, visando minimizar o ônus do processo de elaboração destas.

No capítulo 6 apresenta-se um estudo de caso, onde validou-se o modelo e o *software* na gestão da rede sem fio de uma empresa pública, cuja atividade fim trata-se do ensino superior.

O capítulo 7 apresenta as principais conclusões da dissertação.

2 A MÁ UTILIZAÇÃO DA INTERNET NO AMBIENTE DE TRABALHO

Este capítulo possui como finalidade apresentar o problema de pesquisa da má utilização da Internet. O advento da Internet como fonte principal de comunicação deu origem ao uso massivo de novas tecnologias nas atividades empresariais. Seu emprego tornou-se financeiramente viável, visto que esta pode ser mais rápida e barata que outros meios de comunicação. Outra vantagem proporcionada pela Internet, trata-se da possibilidade dos empregadores em coordenar suas atividades globais de forma remota, com clientes e fornecedores (SHARMA; GUPTA, 2003). Para conhecer outros benefícios, é interessante analisar a pesquisa realizada em (TAN et al., 2010), que averigua um crescimento significativo na região da Malásia após a adoção de tecnologias de comunicação baseadas na Internet por pequenas e médias empresas. A pesquisa mostra que devido a inclusão digital dos empreendimentos, tais organizações tornaram-se passíveis de transações comerciais em escalas globais e consequentemente impactaram positivamente na economia da região.

Tabela 2.1: Principais Benefícios da utilização da Internet nas Empresas. Adaptado de Tan et al., (2010)

Benefícios	**Definição**
Financeiros	Redução do custo em comunicação com consumidores e fornecedores
Velocidade	Maior velocidade no fornecimento de produtos
Eficiência	Aumento da eficiência na coordenação da cadeia de empresas parceiras
Relações de Trabalho	Estabelecimento de relações de trabalho entre parceiros comerciais
Comunicação	Ferramentas para comunicação efetiva com consumidores
Expansão	Oportunidades para novos nichos de mercado

Na Tabela 2.1 observam-se os principais benefícios encontrados pelas empresas devida à adoção da Internet. Nota-se que tais benefícios estão associados com a melhoria na comunicação através de um baixo custo. De forma que ao utilizar essa tecnologia, as empresas conseguem reduzir despesas ao contactar clientes e fornecedores localizados em regiões distantes. Com a queda das barreiras geográficas, proporcionada por essa tecnologia, torna-se possível criar oportunidades para novos nichos de mercado e facilitar o fornecimento de produtos. Em consequência disso, pode-se aumentar a eficiência da organização, resultando em um aumento significativo no capital da empresa.

De muitas maneiras, a Internet pode agregar benefícios as empresas ao prover ferramentas

de comunicação de larga escala à baixo custo. No entanto, surge o interesse em avaliar o efeito da utilização da Internet em relação à produtividade dos trabalhadores. Nota-se que cada vez mais empregados estão acompanhando o preços de suas ações, promoções de passagens aéreas, e-mail pessoal e comunicando-se com seus amigos e parentes durante o horário de trabalho, mesmo que, em alguns casos seus contratantes proíbam (RAMAYAH, 2010). Tais atividades, se praticadas em excesso, resultam em prejuízos para a empresa devida a ineficiência no trabalho.

A ineficiência no trabalho surge em decorrência do baixo desempenho ou da queda de produtividade em um ou vários indivíduos por utilizar de forma incorreta os recursos computacionais. A prática de tal comportamento pode resultar na má realização das tarefas e não cumprimento de prazos. Observa-se assim que a eficiência no trabalho está associada diretamente com a eficiência dos trabalhadores. Desse modo, outro agravante à eficiência no trabalho trata-se da indisponibilidade dos recursos computacionais, devido a má utilização da *Web*, para funcionários que utilizam a Internet para suprir as necessidades da empresa (ANANDARAJAN, 2002).

A má utilização da *Web* é definida como um comportamento voluntário de funcionários que durante o horário de trabalho utilizam recursos computacionais, destinados à organização, para desempenhar atividades pessoais (RAMAYAH, 2010).

Tabela 2.2: Definição de Diferentes Tipos de Abusos na Internet. Adaptado de (SIAU; NAH; TENG, 2002)

Abuso na Internet	**Definição**
Abusos gerais no e-mail	Inclui o envio de Spans, spoofing, disseminação de vírus, propagação de mensagens ofensivas
Uso e acesso não autorizado	Compartilhamento de senhas de acesso sem autorização
Quebra de direitos autorais e Plágio	Uso de software pirata, causando prejuízos para as empresas referente o infringimento de copyright
Postagens em fóruns e new groups	Desperdício de tempo em fóruns com assuntos não relacionados com os interesses da empresa
Transmissão de dados confidenciais	Uso da Internet para disseminação de dados sigilosos da organização
Pornografia	Acesso e navegação e em alguns casos distribuição de conteúdo durante o horário de trabalho
Hacking	Hackear Web sites, promover ataques de negação de serviço e acessar base de dados organizacionais
Download/Upload de arquivos irrelevantes para o trabalho	Utilização de softwares que consomem a largura de banda da empresa em compartilhamento de arquivos ponto a ponto
Uso da Internet como laser	Compras on-line, jogos on-line, programação de viagens, procura de novos empregos, escutar música em rádios on-line, etc
Uso de Proxy Externo	Utilizar provedores de serviços de Internet remotos para encobrir a navegação
Moonlighting	Praticar atividades comerciais no horário de trabalho através da Internet

Na Tabela 2.2, observa-se a definição de diferentes tipos de abusos na Internet. De modo que tais comportamentos estão presentes nos mais diferentes seguimentos empresariais, independente da região onde estes se encontrem (SIAU; NAH; TENG, 2002). Dessa forma, o problema

do uso pessoal da *Web* no ambiente de trabalho tornou-se uma questão global a ser abordada pelas empresas. O estudo relatado em (RAMAYAH, 2010) mostrou que 44% dos 1.000 entrevistados afirmaram gastar em média 2,09 horas do horário de trabalho por dia com o uso pessoal da *Web*. Por sua vez, empresas estimam-se que tais atividades custam 54 bilhões de dólares anualmente em perda de produtividade (YOUNG, 2010).

A busca pela solução de tal problema alcançou escalas globais, de modo que surgiram diversas abordagens visando proporcionar uma proposta que possibilite as empresas beneficiar-se da Internet de forma a não comprometer a produtividade dos funcionários ((ANANDARAJAN, 2002), (GALLETTA; POLAK, 2003) e (PANKO; BEH, 2002)). Apesar de não existir um senso comum quando a classificação dessas abordagens, esta pesquisa baseia-se em (CHOU; SINHA; ZHAO, 2010a) que classifica as principais estratégias contra o comportamento abusivo em eixos. A Tabela 2.3 apresenta essa classificação.

Tabela 2.3: Principais Abordagens Contra a Má Utilização da *Web*. Adaptado de (CHOU; SINHA; ZHAO, 2010a)

Abordagem	**Resultado**
Identificação de Fatores que o Induzem	Utilização da teoria do comportamento planejado.
	Aplicação da teoria do comportamento intrapessoal.
	Dependência e insatisfação no trabalho.
	Depressão, confronto social e distração.
Questões Relacionadas ao Monitoramento	Questões legais relacionadas ao comportamento dos funcionários no trabalho.
Prevenção	Política de Utilização da Internet é a estratégia mais utilizada no trabalho.
	Diretrizes para o desenvolvimento de política eficaz para a Internet.
	Questões e preocupações relacionadas com as atividades preventivas.
	Modelo de medição para avaliar o uso potencial da Web.

Na Tabela 2.3, observa-se que as abordagens presentes na literatura estão associadas a três eixos principais, sendo eles a *Identificação dos Fatores que Afetam o Comportamento Abusivo*, *Questões Relacionadas ao Monitoramento* e a *Prevenção*. Nota-se que no primeiro eixo consideram-se os fatores psicológicos ou sociais relacionados aos empregados, no segundo investigam-se os aspectos legais resultantes da má utilização da Internet por parte dos empregados, enquanto que no terceiro estuda-se a aplicação de medidas que visam evitar a perda de produtividade. Para melhor explanar as peculiaridades de cada eixo, a seção 2.1 apresenta a *Identificação dos Fatores que Afetam o Comportamento Abusivo* , a seção 2.2 o *Monitoramento do Comportamento Abusivo*, enquanto que a seção 2.3 a *Prevenção do Comportamento Abusivo*.

2.1 Identificação dos Fatores que Afetam o Comportamento Abusivo

Essa seção apresenta as peculiaridades presentes nas pesquisas realizadas com o objetivo de identificar os fatores que induzem os funcionários a utilizar à Internet de maneira indevida. As abordagens presentes neste eixo concentram-se em detectar o comportamento abusivo antes da contratação do funcionário, através de testes realizados durante a seleção (CHEN; CHEN; YANG, 2008). Entretanto, por abordar como objeto de estudo o comportamento humano, torna-se necessário compreender alguns aspectos sociológicos que fundamentam à má utilização da *Web*.

Considerando o prisma sociológico, a Internet tende a reduzir o convívio social. De modo que esse processo ocorre como um confinamento do indivíduo em si mesmo para uma comunicação virtual, reduzindo o tempo gasto em interações presenciais (DAVIS; FLETT; BESSER, 2002). Para alguns indivíduos a Internet tem sido uma forma de evitar propositalmente o contato social. De modo que tal tecnologia tornou-se um refúgio contra possíveis ameaças das interações sociais. Por exemplo, um estudante que é muito tímido para realizar uma pergunta ao professor diante de uma classe de alunos, poderia fazê-la por e-mail após a aula, reduzindo efetivamente a ameaça da interação social. Cabe salientar que em relação à área de ensino este fato não é visto negativamente. Pois comprovou-se que, em aulas à distância, tais alunos apresentam maior quantidade e qualidade na participação (RANGEL et al., 2011).

Ainda da mesma forma, um sujeito sensitivo à rejeição poderia relacionar-se através da Internet para evitar magoas emocionais. Percebe-se que para tais indivíduos a comunicação através da Internet poderia auxiliá-los a integrar-se na sociedade. Tais experiências sociais tem motivado a incrementar a dependência dessa tecnologia como meio de comunicação.

No entanto, usuários com esse comportamento apresentam tipicamente dificuldades ocupacionais ou acadêmicas, mais comumente devido aos lapsos de produtividade. Embora muitas organizações empreguem medidas para deter abusos na Internet, muitos funcionários são viciados em certas atividades virtuais e tem pouco controle para não exercê-las no ambiente de trabalho. A prática desse comportamento no local de trabalho passa a ser uma extensão natural da presença dessa prática na vida pessoal desses indivíduos (PEE; WOON; KANKANHALLI, 2008).

Desse modo, um usuário que é acostumado a usar serviços de bate papo em casa responderá sempre instantaneamente para alguma requisição de chats *online* no ambiente de trabalho. Dessa forma, pesquisadores deste eixo tem buscado alternativas com base em teorias compor-

tamentais, capazes de quantificar a tendência desse comportamento em indivíduos. Dentre tais teorias, cabe salientar a *Theory of Planned Behavior* (TPB) (AJZEN, 1991), *Theory of Interpersonal Behavior* (TIB) (TRIANDIS, 1977) e locus de controle (COOVERT; GOLDSTEIN, 1980).

Tanto a teoria do comportamento planejado quanto a do comportamento interpessoal são modelos cognitivos que tentam explicar como a atitude do indivíduo e as normas sociais influenciam suas intenções para agir de maneira particular. Sendo que tais teorias preveem com sucesso diferentes comportamentos humanos em uma variedade de situações (CHUN; BOCK, 2006). Entretanto, a TIB teoriza que, além das construções em TPB, hábito e afeto (emoções) são também aspectos importantes que precisam ser considerados na modelagem de formação de intenção e do comportamento humano (PEE; WOON; KANKANHALLI, 2008).

A TIB postula que, o hábito tem uma influência considerável no comportamento dos indivíduos reais e ainda argumenta que, para muitos comportamentos, o hábito pode ser mais importante do que a intenção na determinação da ação dos indivíduos. A TPB considera apenas o aspecto cognitivo da atitude, enquanto que a TIB considera ambos os aspectos afetivos e cognitivos. O aspecto afetivo é avaliado através do efeto demonstrado ao construir algo, enquanto o aspecto cognitivo é avaliado através da percepção de consequências (PEE; WOON; KANKANHALLI, 2008). Embora a TPB tenha sido amplamente aplicada na compreensão de vários comportamentos ilegais, antiéticos e metanálises, nota-se que a utilização da TIB tem aumentado devido ao seu forte poder preditivo e sua capacidade em proporcionar uma melhor compreensão baseado em contextos onde o hábito e afeto são considerados (TRIANDIS, 1977). Já o emprego da teoria do locus de controle (COOVERT; GOLDSTEIN, 1980), pode contribuir para se averiguar a intensidade de comportamentos viciosos na Internet. Para tal teoria as pessoas são classificadas em dois tipos, as que acreditam que suas próprias ações e esforços estão associadas ao seu sucesso pessoal (locus interno de controle) e as que acreditam que o destino ou sorte são os principais agentes para sua realização pessoal e que estes fatores estão fora do seu próprio controle (locus externo de controle). Para Chen, Chen e Yang (2008), pessoas com locus externo de controle possuem menor propensão à prática de comportamentos viciosos na Internet durante o horário de trabalho.

Toda via, além do locus externo de controle, a autoestima carateriza outro traço determinante para tendência ao vício em Internet de um empregado no ambiente de trabalho (CHEN; CHEN; YANG, 2008). Empregados com alto locus externo de controle são mais comumente

influenciados pelo ambiente externo. Em contrapartida, funcionários com baixa autoestima frequentemente se organizam para utilizar em suas necessidades psicológicas e patológicas. Considerando as habilidades cognitivas dos indivíduos, a escala *online* de cognição (DAVIS; FLETT; BESSER, 2002) classifica o comportamento abusivo em quatro sub escalas: solidão/depressão, diminuição do impulso de controle, conforto social e distração, podendo ser realizado um score mensurável da problemática da utilização da Internet.

Entretanto, as linhas de pesquisas relacionadas ao monitoramento e prevenção partem do pressuposto que não foi identificada a tendência do comportamento abusivo na Internet. De modo que casos onde tornou-se necessário a intervenção do estado para averiguar possíveis crimes digitais, por exemplo, de racismo ou pedofilia tendo evidências comprovando que tais atividades foram executadas por funcionários da instituição através dos recursos computacionais da empresa, despertou o interesse em pesquisadores para criar meios de monitorar o comportamento dos empregados na Internet a fim de diagnosticar a má utilização dessa tecnologia.

2.2 Monitoramento do Comportamento Abusivo

Nesta seção apresentam-se os assuntos pautados no eixo do monitoramento do comportamento abusivo dos funcionários na Internet. As pesquisas classificadas neste eixo contemplam os aspectos legais referente à prática dos empregadores em monitorar seus empregados de modo a não interferir em seus direitos de privacidade como indivíduos. O objetivo é procurar identificar boas práticas com base em causas trabalhistas que possam ser adotadas por empregadores antes de aplicação do monitoramento. Para tal é essencial o entendimento de aspectos legais. Por exemplo, nos Estados Unidos da América, o Decreto da Privacidade das Comunicações Eletrônicas (DPCE) (ECPA, 1986) reconhece o direito das pessoas como indivíduos livres e como tais devem ter sua privacidade respeitada. No entanto, considerando a relação de trabalho, algumas exceções do decreto permitem a prática do monitoramento quanto a utilização dos recursos tecnológicos pertencentes ao empregador. Entretanto, para tornar legal a prática do monitoramento, necessita-se uma concordância formal entre empregadores e empregados.

Nos concordos devem ser expressas tanto normativas de como utilizar à Internet e demais recursos computacionais no trabalho, quanto o consentimento em relação ao monitoramento dos acessos à rede e a auditoria dos dados coletados. Apesar da possibilidade de aplicar essa prática, empregadores devem ser cuidadosos ao adotar tal medida, de forma que mesmo com auditorias internas na empresa comprovando irregularidades quanto a utilização da Internet, dependendo

da situação, algumas cortes podem sentenciar à favor dos empregados. Em (PANKO; BEH, 2002) são apresentados três casos demonstrando esses acontecimentos.

No primeiro, *Smyth vs Pillsbury* , uma corte federal considerou que o empregador poderia demitir Smyth por enviar e-mails não apropriados durante o horário de trabalho. Entretanto, o empregador deveria fazer uma promessa em juízo para não monitorar o e-mail dos funcionários. Com o decorrer do tempo, outro empregado fez comentários ameaçadores sobre seus superiores e colegas através de mensagens eletrônicas. Tais mensagens foram interceptadas pelo empregador, resultando na demissão do funcionário. Sabendo da ocorrência do fato, Smyth recorreu exigindo do empregador uma indenização referente a violação de sua privacidade e quebra da promessa de não monitorar o uso do e-mail. A corte determinou que o empregador não poderia invadir a privacidade de Smyth, visto que o mesmo não possuía motivos razoáveis.

No segundo, *Restuccia vs Burck Technology*, com base em um monitoramento detectou-se que Restuccia utilizou os computadores da empresa para enviar mensagens pessoais, tal funcionária foi demitida por utilizar de forma indevida a Internet. Todavia, a empresa tinha uma política contra bate papos excessivos, mas não contra mensagens pessoais. Restuccia processou a empresa por violação de privacidade. Entretanto, a empresa possuía um acordo formal com a funcionária especificando que os arquivos do computador, incluindo mensagens de e-mail, seriam salvas automaticamente em arquivos de *backup* e estes estariam suscetíveis à auditoria. A corte concluiu que a empresa possuía um motivo razoável para realizar a interceptação, mesmo assim detectou interferência na privacidade da acusada. Visando resumir o julgamento, realizou-se um acordo entre as partes.

Enquanto que no terceiro, *U.S vs Simons*, pode-se estabelecer uma analogia em relação à redução da expectativa de privacidade. Simons, um empregado do governo, exercia a função de contratação de funcionários terceirizados. O governo possuía uma política cujo objetivo era explanar de que forma deveria ser utilizada a Internet e prevenir os empregados de que a utilização dos computadores seria monitorado. De forma que Simons foi instruído a alertar seus subordinados para usar os computadores somente para propósitos do trabalho e que monitoramentos e auditorias poderiam ocorrer. Durante uma auditoria eletrônica, como empregador, Simons foi informado que a companhia de segurança responsável por auditorias descobriu resultados excessivos de conteúdos de pornografia nos computadores dos empregados terceirizados. Através de investigações e pesquisas nos computadores, encontram-se materiais de pornografia infantil, resultando na abertura de uma investigação criminal.

Processado e sentenciado, Simons apelou alegando que a pesquisa durante a auditoria foi uma atitude fora da lei. Mas a corte rejeitou seu argumento, enfatizando que funcionários públicos possuem expectativas de privacidade em seus escritórios ou partes deles, tais como em mesas ou armários de arquivos, mas no caso da utilização de recursos computacionais prevalece os critérios estabelecidos na política de uso. Dessa forma, julgou-se que os empregados não deveriam ter expectativas quanto a privacidade do uso dos computadores, visto que seu supervisor não lhes informou sobre como estes equipamentos deveriam ser utilizados. Desse modo, considerou-se Simons como ciente das evidências e crimes cometidos por seus subordinados. E apesar do reú considerar como intrusão a ação federal em acessar seu disco rígido, considerou-se que a intencionalidade era razoável.

De outra forma, em (TAYLOR; HAGGERTY; GRESTY, 2010) observam-se aspectos legais quanto ao emprego das PUI, sua criação e gerenciamento relacionando-os com a investigação forense. Entre os aspectos legais observados incluem-se a proteção de dados, direitos humanos, poderes de investigação, procedimento de investigação criminal e justiça criminal conforme as leis do Reino Unido. Neste estudo, concluiu-se que conforme as peculiaridades do Reino Unido, para a implantação de PUIs as legislações mais relevantes a serem observadas são referente à proteção de dados e dos direitos humanos. No caso da aplicação de medidas disciplinares quanto a irregularidade do cumprimento das PUIs, os critérios de tais disciplinas devem estar claramente especificados nos regulamentos e termos de utilização dos recursos computacionais da empresa.

Considerando os assuntos pautados neste eixo, notou-se certa sensibilidade referente a observação dos aspectos legais ao empregar técnicas para monitoramento das atividades dos empregados na Internet. Todavia, percebeu-se nesta seção que um dos critérios avaliados pelas cortes é a formalização da clareza de como o empregador julga adequado a utilização dos recursos computacionais. Dessa forma, entende-se que a utilização de medidas preventivas por parte dos empregadores podem ser consideradas uma boa prática por parte dos empregadores. Ao empregar medidas preventivas o empregador pode evitar o comportamento abusivo na Internet, podendo até servir como argumento em sua defesa para justificar a clareza das diretrizes estabelecidas por ele. Desse modo, percebe-se a necessidade de medidas que visam tratar da prática desse comportamento antes que ele ocorra.

2.3 Prevenção do Comportamento Abusivo

Esta seção aborda os assuntos agregados ao eixo da Prevenção do comportamento abusivo dos funcionários na Internet. As pesquisas realizadas neste eixo tem como objetivo propor soluções que evitam a má utilização dos recursos da Internet antes que estes ocorram. Desse modo, tais soluções apresentam contribuições associadas à medidas de controle. Dentre estas medidas, percebem-se maiores esforços nas seguintes áreas: modelos de gestão (CASE; YOUNG, 2001) (YOUNG, 2010) (MAHANEY; LEDERER, 2010) emprego de PUIs (SIAU; NAH; TENG, 2002) (ALAMPAY; HECHANOVA, 2010) (DOHERTY; ANASTASAKIS; FULFORD, 2011) e a utilização de filtros de acesso à Internet (CHOU; SINHA; ZHAO, 2008) (CHOU; SINHA; ZHAO, 2010a) (CHOU; SINHA; ZHAO, 2010b).

Dentre os esforços realizados na área de gestão, cabe destacar o modelo de gestão para utilização proativa da Internet (YOUNG, 2010). O objetivo desse modelo é moldar o comportamento dos empregados que utilizam de forma inadequada os recursos da Internet. Para esse fim, o modelo conta com quatro etapas: *detecção*, *políticas*, *aplicação* e *reabilitação*. A etapa *detecção* é responsável pela identificação do comportamento abusivo dos funcionários na *Web*. A etapa *políticas* representa a elaboração de diretivas de acesso. Em contra partida, a etapa *aplicação* trata do emprego das diretivas estabelecidas. Enquanto que a etapa *reabilitação* inicia-se quando detectado o comportamento abusivo. A teoria que fundamenta esse modelo é de que os funcionários que utilizam a Internet de maneira abusiva possuem um comportamento reativo. Dessa forma, a aplicação de tal modelo visa realizar uma transformação no comportamento dos funcionários, tornando-os proativos.

Já o modelo de Mahaney e Lederer (2010) visa atender os objetivos da gestão de projetos de *software*, aumentando a probabilidade de sucesso de tais projetos. O modelo considera que o sucesso de um projeto depende exclusivamente do cumprimento do prazo e da qualidade do produto. Portanto, objetiva reduzir ao máximo o comportamento abusivo e para isto parte das seguintes hipóteses: Primeira, há necessidade de monitorar o comportamento abusivo; Segunda, a ocorrência do comportamento abusivo está diretamente associada com a probabilidade de sucesso do projeto, de modo que, a menor ocorrência da primeira implica na maior probabilidade da segunda. Com base nessas hipóteses, propôs-se um modelo constituído por quatro etapas, sendo elas: *planejamento*, *delegação de responsabilidades*, *comparação* e *reuniões*. A etapa *planejamento*, objetiva estipular o planejamento do projeto em si, realizar a análise de risco, análise de peculiaridades e montar o gráfico de *Gantt*. A etapa *delegação de responsabilida-*

des, objetiva efetivar o comprometimento dos participantes do projeto com os interesses dos empregadores. Na etapa seguinte, *comparação*, realiza-se uma comparação dos resultados e custos desde a última etapa de planejamento com dados armazenados anteriormente. Enquanto que na etapa *reuniões*, realizam-se reuniões periódicas com objetivo de apresentar os resultados da equipe, dessa forma, através do acompanhamento das atividades realizadas na Internet, conseguiu-se reduzir a má utilização desta tecnologia.

Através de outra perspectiva, pesquisas relacionadas com a aplicação de filtros de acesso à Internet visam prevenir o uso inadequado da Internet (CHOU; SINHA; ZHAO, 2008) (CHOU; SINHA; ZHAO, 2010a) (CHOU; SINHA; ZHAO, 2010b). Os esforços classificados com essa temática objetivam averiguar se as página solicitadas são adequadas com os interesses dos empregadores antes da sua disponibilização. Para isto, utilizam-se filtros de acesso como mediadores entre a rede de computadores da empresa e a Internet. Em (CHOU; SINHA; ZHAO, 2008), propôs-se uma solução baseada na mineração de textos através da extração das *tags Hyper Text Markup Language* (HTML), antes de disponibilizar a página. Aplicou-se técnicas de mineração de texto para classificar o conteúdo da página como apropriado ou não e realizou-se um comparativo dos resultados obtidos com outros modelos na literatura, onde percebeu-se um percentual de verdadeiros positivos de 99% de páginas com conteúdo classificado como inadequado pelos empregadores. No entanto, não houve comparação dos resultados com os de *softwares* comerciais.

Para acurar a eficiência da técnica de classificação de páginas em relação as utilizadas em *softwares* comerciais, Chou, Sinha e Zhao (2010a) realizaram um estudo comparativo entre os três *softwares* proprietários mais utilizados no mercado. Sendo eles: *CYBERSitter* [1] , *Net Nanny* [2] e *CyberPatrol* [3], onde se realizou a mesma configuração nas três ferramentas. Por exemplo, as três apresentavam a opção de restringir o acesso a página de esportes, dessa forma ativou-se esta opção nas três ferramentas. Realizou-se uma coleta de tráfego *Web* com a duração de duas semanas, onde coletou-se dez mil páginas acessadas. Classificou-se estas como apropriada e não-apropriada para o desempenho da profissão de programador, considerando o contexto da indústria de tecnologia da Informação. Onde percebeu-se melhor desempenho no *software CyberPatrol*. Embora notou-se que o mesmo não é capaz de impedir a má utilização da *Web*.

Chou, Sinha e Zhao (2010b) ao considerarem aspectos de desempenho, realizaram um es-

[1] http://www.cybersitter.com/
[2] http://www.netnanny.com/
[3] http://www.cyberpatrol.com/

tudo comparativo entre a técnica de mineração de texto com outra similar chamada *wrapper* (WITTEN; FRANK, 2005). A técnica de mineração de texto possui seus fundamentos na área de inteligência artificial, de modo que relacionado com a má utilização da Internet, o filtro de acesso se tornaria capaz de aprender quais conteúdos não devem ser acessados. A utilização desta técnica requer alto nível de poder computacional, necessitando de outra proposta para treinar a rede neural para aprendizado e apresenta um melhor desempenho considerando o processamento de numerosos documentos. Para sanar esta dificuldade, propôs-se uma seleção híbrida de atributos para classificação de textos associando a técnica *wrapper* com a mineração de textos.

As técnicas apresentadas nesta seção apresentaram técnicas empregadas para previnir a má utilização da Internet. Dentre essas técnicas apresentou-se a aplicação de modelos de gestão e a utilização de regras de acesso incorporadas em filtros de acesso à Internet. Entretanto, apesar de citadas, a seção não explanou sobre a utilização de Políticas de Utilização da Internet.

2.4 Políticas de Utilização da Internet

Políticas de Utilização da Internet são diretrizes definidas pelos empregadores determinando como deve dar-se a utilização da Internet no ambiente de trabalho conforme os interesses dos contratantes. Siau, Nah e Teng (2002) salienta que para criação das diretrizes que compoem a PUI deve-se frisar os valores profissionais da empresa, basear-se no código de ética da utilização de computadores, deixar claro que os recursos computacionais devem ser utilizados conforme os propósitos da empresa, enfatizar que os empregadores tem direitos de monitorar e auditar todos os acessos à Internet, que as diretrizes servem como critério para aplicação de medidas disciplinares e estas devem ser compreendidas formal e informalmente. De maneira similar, Arnesen e Weis(2007) apresenta critérios que determinam a eficácia de uma PUI, salientando os direitos dos empregadores e deveres dos empregados, salientando que não podem:

1. Prejudicar, de qualquer maneira, os negócios ou interesses dos empregadores.
2. Denegrir a imagem da empresa.
3. Enviar, acessar ou arquivar materiais que podem ser considerados discriminatórios, envolvendo alguma forma de assédio ou criando um ambiente de trabalho hostil.
4. Postar conteúdos não relacionados ao trabalho ou envio de spans.
5. Acessar, anexar ou armazenar informações que comprometam a largura de banda da rede.
6. Interferir na produtividade e desempenho, de forma que o uso pessoal da *Web* seja realizado com limites responsáveis.

Em relação aos direitos dos empregadores, citam-se que os critérios impactantes consistem no reconhecimento, por parte dos empregados, de que o empregador tem poderes para:

1. Monitorar a utilização de ambos Internet e e-mail.
2. Armazenar informações deste monitoramento.
3. Bloquear e filtrar materiais classificados como inapropriados, ofensivos ou ameaçador para a segurança da Internet e sistema de e-mail do empregador.
4. Revelar os resultados do monitoramento para todo tipo de auditoria.
5. Aplicar penalidades em caso de violação das PUI.
6. Aplicar ciclos de melhoramento contínuo de tais diretrizes e mudanças quando necessário.
7. Consentir aos empregados direitos para armazenar informações pessoais que não violem a PUI.
8. Acessar e-mails ou arquivos armazenados nos computadores da empresa, incluindo arquivos pessoais, para proteger seus interesses.

Muitos estudos tem sido feito envolvendo esta estratégia, Alampay e Hechanova (2010) examinaram as práticas empregadas nas organizações filipinas referente a utilização de PUIs. O estudo realizado abordou 122 organizações, revelando que dois terços provem acesso à Internet para todos os funcionários e embora a maioria monitorasse a utilização da Internet, menos da metade utilizava PUI. Constatou-se que, em sua maioria, as organizações bloqueiam alguns conteúdos e aplicações *on-line* particularmente relacionados com a pornografia, jogos e redes sociais. Entretanto, apresentam dificuldades em detectar a presença de vírus, devido à *downloads* excessivos de materiais e *chats* na Internet. De modo que, os resultados obtidos sugeriram a necessidade das organizações em articular PUIs, educar os trabalhadores sobre segurança na Internet e formular mecanismos para garantir a integridade do monitoramento dos empregados.

Com o mesmo objetivo, Doherty, Anastasakis e Fulford (2011) exploram a utilização de PUI para prover integridade, confidencialidade e disponibilidade dos recursos computacionais considerado as peculiaridades do ambiente universitário. Primeiramente, detectou-se que o emprego de PUI é a abordagem mais utilizada nas universidades. No entanto, percebeu-se a peculiaridade entre tratar os diversos setores das instituições, visto que não se pode aplicar as mesmas medidas disciplinares em alunos e servidores. Desse modo, os autores analisaram os setores administrativos, de pesquisa e ensino. Onde conclui-se que a aplicação das regras contidas nas PUI em conjunto com uma verificação dos acessos à Internet, deve ser tratado de maneira proativa para promover a segurança da organização.

No entanto esta estratégia apresenta dificuldades quanto ao controle e ao cumprimento das diretrizes (CHOU; SINHA; ZHAO, 2010a). Para contornar essa dificuldade, Rao e Jaeger (2009) aplicam PCAs diretamente em filtros de acesso à Internet. Ao empregar a abordagem baseada em PCA, a granularidade das políticas é um fator essencial para proporcionar aos gerentes a flexibilidade para controlar o acesso a *Web*, mas sem comprometer o potencial do uso da *Web* no ambiente de trabalho (WILSON, 2009).

2.5 Considerações Finais

Este capítulo apresentou que a má utilização da Internet no ambiente de trabalho pode acarretar na perda de produtividade dos funcionários, o que reflete diretamente em receitas financeiras, podendo resultar em sansões legais contra a empresa e ainda denegrir sua imagem perante a sociedade.

Demonstrou-se que existem diversas abordagens para solucionar esse problema, sendo que pode-se classificá-las em três eixos: Identificação, monitoramento e prevenção do comportamento abusivo. No eixo de identificação, agregam-se pesquisas visando identificar a tendência do comportamento abusivo antes da contratação de funcionários. Todavia, no eixo monitoramento estudam-se questões legais quanto à prática de monitorar as atividades dos funcionários na Internet. Enquanto que as pesquisas realizadas na prevenção objetivam propor medidas de controle para evitar a prática do comportamento abusivo.

Observou-se que dentre as estratégias mais utilizadas, a mais empregada é a prevenção da má utilização da Internet através de PUIs. No entanto, citou-se que apesar de sua larga utilização, o emprego dessa estratégia apresenta dificuldades quanto ao controle do cumprimento das diretrizes estabelecidas. Para contornar essa dificuldade, alguns autores propõe a utilização de PCAs atuando diretamente em filtros de acesso à Internet. Entretanto, ao utilizar a abordagem baseada em PCA, a granularidade é um fator essencial para proporcionar que a Internet seja utilizada de maneira controlada, mas sem comprometer os benefícios gerados pela utilização dessa tecnologia.

3 POLÍTICAS DE CONTROLE DE ACESSO

Esse capítulo tem como objetivo averiguar qual abordagem de Política de Controle de Acesso (PCA) apresenta a granularidade mais apropriada para as peculiaridades do problema da má utilização da *Web*. Para isto, a seção 3.1 demonstra qual o papel das PCAs através da perspectiva da Gestão da Segurança da Informação (GSI), bem como sua aplicabilidade ao controlar acessos indevidos à *Web*. As seções 3.2, 3.4 e 3.4 apresentam, respectivamente, as propriedades das PCAs discricionárias, baseadas em perfis e sensíveis à atributos contextuais. A seção 3.5 apresenta as considerações finais do capítulo.

3.1 Gestão da Segurança da Informação

Para definir o papel das PCAs através da GSI necessita-se primeiramente entender qual o objetivo da GSI. A GSI objetiva gerir a segurança aplicada as informações de uma organização. De modo que para isto, visa garantir as seguintes propriedades às informações geridas: integridade, disponibilidade e confidencialidade. Para melhor apresentar esses conceitos, a Tabela 3.1 sumariza estas propriedades.

Tabela 3.1: Principais Propriedades da Gestão da Segurança da Informação. Adaptado de (SAMARATI; VIMERCATI, 2001)

Propriedade	**Definição**
Integridade	Provê a garantia da consistência dos dados gerenciados
Disponibilidade	Garante que quando solicitados, os dados estarão aptos para serem acessados por entidades autorizadas
Confidencialidade	Objetiva prover que os dados sejam disponibilizados somente para pessoas autorizadas

Em termos de acesso *Web*, a integridade pode ser entendida como a garantia de que o conteúdo HTML exibido no navegador condiz com a *Uniform Resource Locator* (URL) solicitada e a disponibilidade como a certeza de que a banda de Internet sempre estará disponível para utilização quando solicitada para atividades relacionadas com o interesse da empresa. Já a confidencialidade pode ser entendida como a garantia de que somente os sites classificados como relevantes aos interesses da empresa estarão disponíveis para os funcionários.

Em virtude do conceito de GSI e suas respectivas propriedades, cabe agora identificar sua relação com as PCAs. Para isto, torna-se necessária uma revisão sobre o conceito de controle de acesso. Desse modo, retomando a definição de GSI, percebe-se que para cumprimento de suas

propriedades, a GSI necessita que todo acesso ao sistema e/ou seus recursos sejam controlados. De maneira que somente acessos autorizados venham ser efetivados. Este processo recebe o nome de controle de acesso (SAMARATI; VIMERCATI, 2001). Dessa forma, tendo definido o conceito de controle de acesso, percebe-se a necessidade de regular como se dará o acesso, ou seja, precisa-se criar regras explicitando como os recursos da Internet serão acessados e por quem. Este processo chama-se política de acesso. Considerando a aplicação de políticas de acesso, torna-se necessário o entendimento de que são modelos de segurança, mecanismos de segurança, políticas de segurança e PCAs. A Tabela 3.2 apresenta esses conceitos e definições.

Tabela 3.2: Principais Elementos da Gestão da Segurança da Informação. Adaptado de (SAMARATI; VIMERCATI, 2001)

Elemento	**Definição**
Modelo de Segurança	Provê uma representação formal da segurança e funcionamento do controle de acesso.
Mecanismo de Segurança	Define em baixo nível (hardware e software) funções que implementam os controles impostos pelas políticas.
Política de Segurança	Define em alto nível (diretrizes) regras que determinam como o controle de acesso deve ser regulado.
PCA	Representa em nível de linguagem de programação as regras interpretadas pelo mecanismo de controle de acesso. Sendo que estas normalmente baseiam-se nas políticas de segurança.

Na Tabela 3.2 percebem-se os principais elementos da GSI, sendo eles: modelo de segurança, mecanismo de segurança, política de segurança e PCA. Relacionando esses conceitos com o problema da má utilização da *Web*, o modelo de segurança pode ser entendido como o projeto adotado pela empresa determinando como se dará o controle de acesso. De outra forma, o mecanismo de segurança pode ser interpretado como o filtro de acesso à Internet, ou seja, o software empregado para bloquear os acessos indesejados. Já a política de segurança, assim como a PUI, são diretrizes formalmente especificadas em documentos com objetivo de orientar os funcionários. Enquanto que, segundo (2001), as PCAs traduzem diretrizes das políticas de segurança para uma linguagem compreensível ao filtro de acesso, a fim de regular o acesso conforme os interesses dos empregadores. Dessa forma, pode-se entender que o papel das PCAs através da GSI é como de uma interface onde os empregadores podem definir suas regras de acesso à Internet a fim de serem aplicadas por filtros de acesso.

Com base no papel das PCAs em relação à GSI, pode se perceber que PCAs mal elaboradas podem comprometer a produtividade dos funcionários ao serem muitos restritivas ou demasiadamente permissivas, salientando a necessidade pela busca de uma abordagem de PCAs que seja capaz de representar as peculiaridades dos mais diversos seguimentos de negócio sem pre-

judicar a produtividade dos trabalhadores. Com uma granularidade fina, ou seja, regras de acesso ricas em informações, pode-se criar regras personalizadas para cada tipo de situação da empresa, permitindo uma melhor utilização da Internet.

Para melhor entender a necessidade de utilizar PCAs com granularidade fina em filtros de acesso à Internet, considere o exemplo de uma instituição de ensino de nível superior, onde sua atividade fim é o processo de ensino/aprendizado. Por se tratar de uma universidade, além das atividades administrativas e de ensino nesta deve haver atividades de pesquisa. Note que para prestar um ensino de qualidade, não pode-se aplicar regras rígidas que impeçam as pesquisas dos alunos. Todavia também não se pode deixar o acesso liberado ao ponto de permitir a utilização inapropriada desses recursos por parte de funcionários e alunos.

Para apresentar as principais técnicas de PCAs, a fim de encontrar a que melhor se ajuste em uma instituição de ensino, a Tabela 3.3 resume o conceito sobre as PCAs discricionárias, baseadas em perfis e sensíveis ao contexto.

Tabela 3.3: Políticas de Controle de Acesso, Abordagens Tradicionais. Adaptado de (NIST, 2009)

Abordagem	**Definição**
Discricionárias	Forma mais básica de controle de acesso. De modo que associa permissões diretamente à usuários e recursos gerenciados. Por basear-se em listas de controle de acesso, apresenta difícil administração.
Baseadas em Perfis	Apresenta facilidades administrativas devida a inserção de um elemento intermediário entre os usuários e recursos gerenciados, o perfil. De forma que, ao contrário do discricionário, as permissões são atribuídas aos perfis e os perfis são associados aos usuários. Devida a essa peculiaridade, esse modelo também é conhecido como baseado em perfis.
Sensíveis ao Contexto	Expressa em suas regras de acesso atributos contextuais indicando dinamicidade, tais como tempo e localização. Sendo plausível de configuração conforme as peculiaridades do ambiente adotado.

Na Tabela 3.3 apresentam-se as abordagens tradicionais de PCAs, sendo elas: discricionárias, baseadas em perfis e sensíveis ao contexto. As discricionárias representam a forma mais básica de controle de acesso e relacionam as permissões de acesso diretamente a usuários e recursos gerenciados através de listas de controle de acesso. As PCAs baseadas em perfis (SANDHU et al., 1996), apresentam maiores facilidades administrativas, visto que neste modelo insere-se o perfil como um elemento intermediário entre os usuários e recursos gerenciados, o que permite associar as permissões de acesso aos perfis e os usuários com estes perfis. Já as sensíveis ao contexto expressam em suas regras de acesso atributos contextuais, tais como tempo e localização, que necessitam ser avaliados para a concessão da permissão.

Dentre essas abordagens, a que apresenta granularidade mais fina é a abordagem sensível ao contexto. Para demonstrar como se chegou a esta conclusão, consideremos as seguintes peculiaridades presentes nas universidades que devem ser considerados ao aplicar PCAs: *a)* A má utilização da Internet em sala de aula pode prejudicar a aprendizagem, portanto, torna-se interessante utilizar PCAs capazes de expressar particularidades do meio acadêmico, tais como a habilitação dinâmica de perfis e restrições temporáriais; *b)* Algumas atividades exercidas na universidade precisam ter acesso à conteúdos da *Web* que muitas vezes são utilizados para comportamentos não produtivos, tais como redes sociais; e *c)* Uma universidade pode assumir características de um ambiente dinâmico, ou seja, um sujeito pode exercer funções distintas conforme sua localização e horário. Desse modo, considerando o tratamento dessas peculiaridades, a seção 3.2 apresenta como a abordagem discricionária se aplicaria a este problema, a seção 3.3 como a abordagem baseada em perfis se aplica, e a seção 3.4 como as sensíveis ao contexto se aplicam.

3.2 Discricionárias

Políticas de Controle de Acesso Discricionárias, ou pertencentes ao modelo *Discretionary Access Control* (DAC), constituem a forma mais elementar de PCA (BARRERA et al., 2010). Políticas DAC baseiam-se na identidade dos sujeitos e objetos para regular o acesso, delimitando o que os requisitantes de acesso podem fazer. Dessa forma, o gerenciamento da informação empregado por essa abordagem dá-se através da associação de sujeitos e permissões associados a um objeto ou recurso computacional, onde torna-se necessário criar regras específicas para cada recurso. O motivo de chamarem as PCAs deste modelo de discricionária dá-se pelo fato de um sujeito dono de um recurso pode repassar direitos de acessos a este recurso para outros sujeitos.

Para criar uma PCA do tipo DAC precisa-se associar sujeitos e permissões à um objeto ou recurso computacional. Portanto, considerando o ambiente acadêmico, para um professor disponibilizar pesquisas no site do *Google*, pode-se identificar os sujeitos como os alunos, a permissão de acesso *Web* e o objeto que se quer controlar o acesso como o site do *Google*. Deste modo, a Política 3.1 ilustra como uma política DAC associa esses sujeitos e permissões ao recurso.

```
1 <Politica DAC>
2   <Sujeito>
3     - Paulo
4     - Pedro
5     - João
```

```
6     </Sujeito>
7     <Objeto>
8       - http://www.google.com.br/
9     </Objeto>
10    <Permissão>
11      - ACESSO WEB
12    </Permissão>
13  </Politica DAC>
```

Política 3.1: Política DAC que Permite Acesso ao Site do Google

Na Política 3.1, pode-se observar que entre as *tags* Sujeito encontram-se a identidade dos alunos, neste caso seus nomes. Em Objeto, a URL do site do *Google*. Enquanto que na Permissão, a liberação do acesso. Como se pode ver, é plausível afirmar que políticas DAC cumprem a primeira particularidade apresentada quanto a aplicação de PCAs em uma empresa cuja atividade fim é o ensino universitário, de forma que cabe agora averiguar a aplicabilidade dessa quanto a segunda e terceira. A segunda particularidade diz respeito a possibilidade de conceder permissões particulares à algumas atividades estratégicas de alguns setores. Considerando a mesma estrutura apresentada na Política 3.1, pode-se afirmar a possibilidade da especificação de uma PCA que permita determinado sujeito à acessar uma URL tal como a do *Facebook*.

Todavia, percebe-se que em alguns casos funcionários da universidades, em determinado momento, assumem o papel de aluno dentro da instituição. Assim como determinados professores assumem, em determinados momentos, papéis de cargos administrativos, tais como reitor e diretor de centro ou coordenador de curso. Sendo que em cada um desses perfis (aluno, professor, coordenador de curso) necessitam-se de permissões heterogêneas. Suponha um programador da universidade que desenvolva interfaces *Web*. Devido ao desempenho dessa atividade pode ser interessante durante seu horário de trabalho que este profissional tenha acesso à redes sociais. Todavia, ao assumir o papel de aluno, acessar esses conteúdos podem comprometer seu desempenho quanto a aprendizagem. Dessa forma, nota-se que apesar de cumprir a primeira e segunda particularidade, a proposta DAC não representa as dinamicidades presentes no meio acadêmico universitário.

Além do não cumprimento da terceira particularidade, outra dificuldade apresentada por essa abordagem trata-se da dificuldade administrativa. Visto que devido à associação dos identificadores dos sujeitos juntamente ao recurso computacional e sua respectiva permissão, em caso de mudanças organizacionais, em ambientes com diversos recursos, corre-se o risco de que administradores de sistemas esqueçam de revogar as permissões de acesso em todos os recursos computacionais. Resultando em sujeitos que não fazem mais parte da instituição continuem com alguns privilégios às informações gerenciadas, no caso a rede da empresa.

3.3 Baseadas em Perfis

Políticas de controle de acesso baseadas em perfis, ou provenientes do modelo *Role-Based Access Control* (RBAC) (FERRAIOLO et al., 2001), objetivam sanar a dificuldade apresentada no modelo DAC quanto à administração das políticas. Esse aprimoramento dá-se através da inclusão do perfil como integrante da PCA. Dessa forma, ao invés de associar os identificadores dos sujeitos aos recursos computacionais e suas respectivas permissões, associa-se primeiramente o perfil com seus respectivos objetos e permissões e em seguida, relacionam-se os identificadores dos sujeitos que exercem tais perfis dentro da instituição. Dessa forma, no caso de ocorrência de mudanças organizacionais, não corre-se o risco do administrador esquecer determinados privilégios. Visto que, neste caso desassocia-se o sujeito ao perfil, e não aos objetos e permissões (NIST, 2009).

Sanada a dificuldade administrativa, resta agora averiguar se essa abordagem de PCA é capaz de representar as peculiaridades do ambiente universitário. Dessa forma, como visto anteriormente, precisa-se identificar os perfis provenientes desse segmento de negócio e suas respectivas permissões. Para facilitar esse entendimento, demonstra-se uma possível relação entre a classificação de URLs e os sujeitos permitidos a acessá-los (Tabela 3.4).

Tabela 3.4: Relação entre Classificação de URL e Sujeitos Autorizados

Classificação de URLs	**Sujeitos Autorizados**
Domínio da Universidade	*Todos*
Redes Sociais	*Alunos de Publicidade*
Mensagens Instantâneas	*Funcionários da Universidade*
Wikis	*Programadores*
Sites de Pesquisa	*Alunos da Universidade*
Sites Inapropriados	*Ninguém (Política "mundo fechado", onde tudo o que não for explicitamente permitido é negado por padrão.)*

Na Tabela 3.4 observa-se a relação entre uma possível classificação de URLs com sujeitos autorizados à acessá-los. Percebe-se que essa relação fundamenta-se com as peculiaridades apresentadas em instituições de ensino universitário, visto que os sujeitos autorizados apresentados nessa relação pertencem a esse domínio. Devido ao fato que o RBAC trata-se de uma evolução do modelo DAC, consequentemente a mesma capacidade de representação de políticas DAC se aplica às RBAC. Desse modo, considere a criação de uma PCA RBAC que objetiva prover a terceira particularidade das instituições universitárias citadas anteriormente.

Para este fim, precisa-se considerar perfis que representem as diversas funções desempe-

nhadas neste segmento empresarial, de modo que estes perfis abranjam tanto à área de ensino, pesquisa e administrativa. Dessa forma, tendo como base à área de ensino cabe considerar os perfis de aluno e professor de cada disciplina ministrada. Em relação à pesquisa, cabe destacar a função do pesquisador de iniciação científica, aluno de mestrado e orientador. Além disso, do ponto de vista administrativo, torna-se interessante considerar as possíveis funções exercidas por professores, como de coordenador de curso, diretor do centro e demais cargos na reitoria. Porém, existem funções administrativas exercidas por demais profissionais, não professores, tais como publicitários, programadores, chefes de setor, entre outros. Para demonstrar o contraste entre as diferentes funções exercidas em uma instituição universitárias, resumimos alguns perfis na Tabela 3.5.

Tabela 3.5: Perfis RBAC Para uma Instituição de Ensino

Perfil
Aluno Irregular
Aluno da disciplina de Sistemas Distribuídos
Programador de Interfaces Web
Professor do curso de Ciência da Computação
Professor da disciplina de Sistemas Distribuídos *Diretor de Centro*

Na Tabela 3.5, nota-se que os perfis considerados contrastantes são de Aluno Irregular, aluno de uma disciplina em vigência, no caso Sistemas Distribuídos, programador de Interfaces *Web*, professor de um curso ofertado, no caso Ciência da Computação e Diretor de Centro. O objetivo da escolha desses perfis deu-se para demonstrar como as políticas RBAC possibilitam a especificação de PCAs por funções e tais funções podem ser derivadas de um perfil principal, tal como aluno irregular e aluno da disciplina de Sistemas Distribuídos deriva de aluno, Programador de Interfaces *Web* e professor derivam de Funcionário. Assim como Professor do curso de Ciência da Computação e Diretor de Centro derivam de professor.

Tendo definido os perfis, resta agora ao administrador definir quais permissões são relevantes a cada perfil. Como dito anteriormente, o objetivo de investigar estratégias baseadas em PCAs dá-se para possibilitar uma potencialização no acesso à Internet. Dessa forma, o foco principal é permitir peculiaridades presentes em ambientes empresariais que utilizam essa tecnologia. Com base nisto, pensou-se em possíveis permissões de acesso à Internet. A Tabela 3.6 apresentam essas permissões.

Na Tabela 3.6, observa-se que está sendo considerado a possibilidade dos administradores

Tabela 3.6: Permissões RBAC Para Acesso à Rede Sem Fio de uma Instituição de Ensino

Permissão
Aluno Irregular pode acessar o Domínio da Universidade
Aluno de Sistemas Distribuídos pode acessar Sites de Pesquisa
Programador de Interfaces Web pode acessar Redes Sociais
Professor de Ciência da Computação pode acessar Sistema On-line de Presenças
Funcionário da Universidade pode enviar Mensagens Instantâneas

acharem conveniente que alunos irregulares tenham acesso mais restrito que os regulares e que o professor da disciplina de Sistemas Distribuídos permite aos seus alunos acessar somente sites de pesquisa. Considerou-se também a necessidade do programador de Interfaces *Web* ter acesso à redes sociais e ainda que um professor pode acessar um sistema de acompanhamento de presenças eletrônico, disponível no site da universidade. Enquanto que os funcionários da universidade tem permissões para se comunicarem entre si através de mensagens instantâneas, reduzindo despesas telefônicas.

Tendo definido os perfis, permissões e como estas se relacionam com os sujeitos do ambiente universitário, resta agora definir políticas RBAC propriamente ditas. Desse modo, considere a necessidade da criação de uma política restritiva, ou seja, que restrinja os acessos indesejados de um aluno à Internet. Para ilustrar essa PCA, a Política 3.2 apresenta como esta poderia ser representada.

```
1  <Politica RBAC>
2    <Sujeito>
3      - Perfil = Aluno de Sistemas Distribuídos
4    </Sujeito>
5    <Objeto>
6      - Sites Inapropriados
7    </Objeto>
8    <Permissao>
9      - NEGADA
10   </Permissao>
11 </Politica RBAC>
```

Política 3.2: Política RBAC que Proíbe o Acesso à Sites Considerados Inapropriados

Na Política 3.2, percebe-se que o perfil *Aluno de Sistemas Distribuídos* abstrai a identificação dos sujeitos, diferentemente das políticas DAC. Entre as *tags* Objeto, pode-se notar que a regra foi formulada para atingir toda uma classificação de sites considerados irrelevantes para disciplina. No entanto sua representação na política apresenta como uma classificação *Sites Inapropriados*. Da mesma forma, poderia ser criada uma política permissiva, isto é, uma PCA que expresse regras permissivas quanto à Utilização da Internet em horário de aula. Visando representar essa PCA, ilustrou-se a Política 3.3.

```
<Politica RBAC>
  <Sujeito>
    - Perfil = Aluno de Sistemas Distribuídos
  </Sujeito>
  <Objeto>
    - Sites de Pesquisa
  </Objeto>
  <Permissão>
    - CONCEDIDA
  </Permissão>
</Politica RBAC>
```

Política 3.3: Política RBAC que Permite o Acesso à Sites de Pesquisa

Na Política 3.3 observa-se uma política capaz de permitir aos alunos da Disciplina de Sistemas Distribuídos acessarem os sites classificados pelo professor como de pesquisa. Percebe-se que políticas RBAC, além da facilidade administrativa, proporcionam capacidade para representar diversos segmentos empresariais por atribuir ao perfil uma associação indireta entre identificadores de usuários, objetos e permissões.

Dessa forma, considerando as peculiaridades citadas anteriormente, pode-se dizer que as Políticas 3.2 e 3.3 representam a primeira peculiaridade, isto é, que uma estratégia de PCA deve expressar particularidades do meio acadêmico. Assumindo que a necessidade de acesso à sites de pesquisa durante as aulas de Sistemas Distribuídos é uma particularidade do ambiente universitário, logo podemos afirmar que PCAs RBAC contemplam esse critério. Resta ainda averiguar sua aplicabilidade quanto a segunda e terceira particularidade.

Na segunda particularidade, diz-se que é necessário para algumas atividades desempenhadas na universidade o acesso à conteúdos da *Web* muitas vezes utilizados em comportamentos improdutivos, tais como redes sociais. Tendo como base essa premissa, a Política 3.4 objetiva ilustrar como dar-se-ia a representação RBAC para essa PCA.

```
<Politica RBAC>
  <Sujeito>
    - Perfil = Desenvolvedor de Interfaces Web
  </Sujeito>
  <Objeto>
    - Redes Sociais
  </Objeto>
  <Permissão>
    - CONCEDIDA
  </Permissão>
</Politica RBAC>
```

Política 3.4: Política RBAC que Permite o Acesso à Redes Sociais

Na Política 3.4, nota-se a criação do perfil desenvolvedor de Interfaces *Web*, que como explicado anteriormente, pode necessitar acessar redes sociais para basear-se na usabilidade proporcionada em tais recursos para adaptá-la ao sistemas que ele desenvolve. Portanto, percebe-se

que utilizou-se a classificação Redes Sociais como um conjunto de URLs de redes sociais definidas pelo respectivo gerente desse funcionário. Note que o exemplo do desenvolvedor de interfaces poderia ser aplicado a diversos outros casos. Por exemplo, à alunos de música poderiam necessitar de acesso à conteúdos de áudio, para alunos de publicidade que poderiam precisam ter acesso à redes sociais ou devido a ampliação do uso de redes no contexto educacional alunos necessitam acessar o blog do professor, da displina ou utilizar ferramentas de colaboração no desenvolvimento de textos e projetos. Além disso, para um gerente de software da universidade que necessitasse de acesso à mensagens instantâneas para levantar requisitos de um projeto. Assumindo que esses casos podem ser considerados como peculiaridades do ambiente universitário que necessitam de acesso diferenciado à Internet por razões peculiares, por conseguinte pode-se afirmar que políticas RBAC contemplam também o segundo critério. De modo que resta-nos comprovar sua aplicabilidade quanto à terceira particularidade.

A terceira particularidade afirma que uma universidade pode assumir características de um ambiente dinâmico. De forma que, um sujeito pode exercer funções distintas conforme sua localização e horário. Como visto anteriormente, políticas RBAC são capazes de representar funções distintas de uma organização através do emprego do elemento perfil. Todavia, não são mencionadas implicações quanto a especificação de critérios dinâmicos para ativação desse perfil, tais como localização do indivíduo e horário do acesso. Desse modo, considerando que RBAC não possui capacidade da especificação de critérios dinâmicos para ativação do perfil, pode-se concluir que, apesar dos diversos benefícios proporcionados, essa abordagem não contempla a terceira particularidade.

3.4 Sensíveis à Atributos Contextuais

Políticas de controle de acesso sensíveis à atributos contextuais, ou baseadas em atributos, visam estender o modelo de políticas baseado em perfis por considerar atributos dinâmicos, tais como tempo e localização (YUAN; TONG, 2005). Os atributos dinâmicos avaliados por esse modelo, estão associados normalmente a uma entidade de contexto. Uma entidade de contexto trata-se da representação de uma entidade envolvida durante uma requisição de acesso, tais como o sujeito que realiza a solicitação, o objeto requisitado e a representação do ambiente que os envolve (MACEDO; NUNES; BANDEIRA, 2010).

Ciente de que este modelo estende o modelo baseado em perfis, ampliando sua capacidade representativa, entende-se implicitamente que como a abordagem baseada em perfis contem-

plou a primeira e segunda peculiaridade, não sendo necessário representá-las novamente. Em virtude disto, essa seção se concentra na terceira peculiaridade, a de que um sujeito pode exercer funções distintas conforme sua localização e horário de acesso.

Para isto, baseados nos exemplos anteriores, considere o caso de um funcionário do centro de processamento de dados que exerça a função de desenvolvedor de interfaces *Web* e que deve documentar seu código em uma Wiki do projeto, sendo que no mesmo período torna-se interessante que este tenha acesso à sites de redes sociais. Considere também que este mesmo funcionário possua contrato de vinte horas de trabalho, cumprindo-as em meio expediente durante o turno da tarde. Finalmente, suponha que este sujeito esteja cursando Ciência da Computação, sendo que suas aulas ocorram no período da manhã e que na quarta-feira, seu professor de sistemas distribuídos considere inapropriado para suas aulas que os alunos acessem sites de redes sociais e salas de bate papo. Todavia, o professor considera de fundamental importância o acesso à fóruns *on-line* sobre sua disciplina e tolere o acesso ao domínio interno da universidade.

Com este cenário percebe-se a necessidade da criação de dois perfis: desenvolvedor de interfaces *Web* e aluno de sistemas distribuídos. Todavia, percebe-se que se não houverem restrições temporais quanto a ativação dos perfis, corre-se o risco de que este sujeito tenha acessos à sites de redes sociais durante o período em que assiste aulas da disciplina de sistemas distribuídos, um comportamento considerado inapropriado pelo professor. Para demonstrar como as PCAs sensíveis ao contexto podem solucionar este impasse, vamos considerar primeiramente uma política que atenda os requisitos de acesso durante o expediente de trabalho. A Política 3.5 apresenta essa representação.

```
<Politica CONTEXTUAL>
  <Sujeito>
    - Perfil = Desenvolvedor de Interfaces Web
    - Local = Centro de Processamento de dados
    - (Horário Atual >= 14:00)
      E
      (Horário Atual <= 18:30)
    - (Dia da Semana = Segunda-feira) OU (Dia da Semana = Terça
      -feira)
      OU
      (Dia da Semana = Quarta-feira) OU (Dia da Semana = Quinta-
        feira)
      OU
      (Dia da Semana = Sexta-feira)
  </Sujeito>
  <Objeto>
    - (Conteúdo = Redes Sociais)
      OU
      (Conteúdo = Wikis)
  </Objeto>
  <Permissão>
    - CONCEDIDA
```

```
21    </Permissão>
22  </Politica CONTEXTUAL>
```

Política 3.5: Política com Informações Contextuais que Permite o Acesso à Redes Sociais e Wikis durante às Tardes

Na Política 3.5, percebe-se que o perfil *Desenvolvedor de Interfaces Web* é ativado somente no local do centro de processamento de dados, entre às 14 e 18 horas e das segundas às sextas-feiras. Sendo que, tal política lhes dá direito, de forma permissiva, a sites cujo conteúdo está relacionado com redes sociais e Wikis. Dessa forma, pode-se perceber que a Política 3.5 expressa os critérios necessários para realização das tarefas do ambiente de trabalho. Cabe agora, demonstrar como a abordagem baseada em atributos contextuais pode solucionar o problema relacionado com as aulas. A Política 3.6 apresenta a política permissiva quanto ao comportamento considerado apropriado pelo professor de sistemas distribuídos.

```
1  <Politica CONTEXTUAL>
2    <Sujeito>
3      - Perfil = Aluno de Sistemas Distribuídos
4      - Local = Sala 321
5      - Centro = Centro de Tecnologia
6      - (Horário Atual >= 07:30)
7        E
8       (Horário Atual <= 12:00)
9      - (Dia da Semana = Quarta-feira)
10   </Sujeito>
11   <Objeto>
12     - (Conteúdo = Fóruns de Pesquisa)
13       OU
14      (Conteúdo = Domínio da Universidade)
15   </Objeto>
16   <Permissão>
17     - CONCEDIDA
18   </Permissão>
19 </Politica CONTEXTUAL>
```

Política 3.6: Política com Informações Contextuais que Permite Acesso aos Domínios da Universidade e Fóruns de Pesquisa Durante às Manhãs

Na Política 3.6, pode-se notar a utilização do perfil *Aluno de Sistemas Distribuídos* para classificar os indivíduos para os quais a regra se aplica. Observa-se que a regra é válida exclusivamente para a sala 321 localizada no Centro de Tecnologia. De modo que esta entra em vigência somente nas quartas-feiras nos horários entre 07:30 às 12:00, permitindo acessos à fóruns de pesquisa e ao domínio da Universidade. Tendo definido a política responsável por permitir o acesso aos sites considerados apropriados pelo professor e suas respectivas condições de aplicabilidade, cabe agora definir uma PCA que restrinja o acesso aos recursos considerados inapropriados pelo professor. Dessa maneira, a Política 3.7 apresenta a PCA restritiva.

```
1  <Politica CONTEXTUAL>
2    <Sujeito>
3      - Perfil = Aluno de Sistemas Distribuídos
4      - Local = Sala 321
```

```
5       - Centro = Centro de Tecnologia
6       - (Horário Atual >= 07:30)
7         E
8         (Horário Atual <= 12:00)
9       - (Dia da Semana = Quarta-feira)
10    </Sujeito>
11    <Objeto>
12      - (Conteúdo = Redes Sociais)
13        OU
14        (Conteúdo = Salas de Bate Papo)
15    </Objeto>
16    <Permissão>
17      - NEGADA
18    </Permissão>
19  </Politica CONTEXTUAL>
```

Política 3.7: Política com Informações Contextuais Restritiva à Redes Sociais e Salas de Bate Papo Durante os Turnos da Manhã

Na Política 3.7, percebe-se que as condições para ativação da política localizadas entre as *tags* Sujeito são idênticas as da Política 3.6. Todavia, notam-se alterações quanto aos recursos gerenciados e a autorização especificada. Quanto aos recursos, pode-se notar que a classificação dos sites especificados dizem respeito à conteúdos classificados como proveniente de redes sociais e salas de bate-papo. Enquanto que a permissão expressa, ao contrário da Política 3.6, torna-se negada.

Considerando que o exemplo citado pode-se aplicar em diversos outros casos, tais como para professores que em dado momento assumem funções administrativas, para alunos de graduação que dependendo da circunstância exercem o papel de pesquisador de iniciação científica ou ainda mestrandos que em determinado instante assumem papel de monitores de disciplinas. Logo, pode-se afirmar que PCAs sensíveis à atributos contextuais são capazes de representar a dinamicidade do ambiente universitário citado na peculiaridade *c*. De modo que, como demonstrou-se as peculiaridades *a* e *b* através das PCAs baseadas em perfis, pode-se afirmar que as PCAs sensíveis à atributos contextuais contempla todos as peculiaridades do ambiente universitário. Dessa forma, provê a granularidade apropriada quanto ao emprego dessas políticas como medida preventiva quanto a má utilização da *Web* em um ambiente real.

3.5 Considerações Finais

As PCAs discricionárias constituem a forma mais elementar de controle de acesso, relacionando permissão diretamente a usuários e recursos. Como resultado, apresenta dificuldades administrativas e granularidade grossa na representação de regras de controle de acesso. Já, PCAs baseadas em perfis facilitam a gestão, pois possibilitam categorizar os usuários e manipular regras com mais eficácia, e as PCAs sensíveis à atributos contextuais apresentam granularidade

fina, possibilitando representar critérios dinâmicos tais como localização e horários de acesso. A representação de atributos com granularidade fina, incluindo a representação de perfis, amplia significativamente a possibilidade de uso de PCAs.

Por outro lado, como a Internet representa um ambiente altamente dinâmico, ou seja, constantemente milhões de documentos são inseridos para disponibilização e outros milhões são atualizados ou tirados de funcionamento, percebem-se desafios na aplicação de um modelo de gestão baseado em PCAs como forma de conter a má utilização da Internet. O principal desafio é a necessidade de granularidade fina para definir regras de acesso efetivas e a possibilidade de que tais PCAs tornem-se obsoletas e onerem a elaboração e manutenção de tais políticas. Fica então evidente que se as políticas não forem gerenciadas periodicamente, dentro de pouco tempo elas se encontraram desatualizadas e obsoletas, principalmente se elas forem especificadas com granularidade fina. Percebe-se também que para a especificação de PCAs sensíveis a atributos contextuais torna-se necessário um nível de conhecimento técnico elevado, o que torna a tarefa de administração uma atividade para pessoas especializadas, podendo demandar custos extras para organização.

Em síntese, realizar a prevenção do uso inadequado da Web através de uma abordagem baseada em PCAs demanda mecanismos de controle de acesso de granularidade fina, para poder controlar acesso a conteúdos web, e um modelo de gestão que estimule a revisão periódica das regras de acesso e evite altos custos de manutenção.

4 MODELO DE GESTÃO PARA PREVENÇÃO DA MÁ UTILIZAÇÃO DA WEB

Neste capítulo propõe-se um Modelo de Gestão para Prevenção da Má Utilização da *Web*. Pode-se citar como característica do modelo proposto o fato de que este baseia-se nas PUIs, estratégia preventiva mais empregada, para sanar as dificuldades quanto ao cumprimento das diretrizes estabelecidas, bem como que ele utilizara PCAs sensíveis à atributos contextuais e gerencia essas políticas através de um ciclo de melhoramento contínuo. A adoção de um ciclo de melhoria possibilita uma gestão com o envolvimento dos recursos humanos da empresa, incrementando a cultura da segurança organizacional.

O modelo baseia-se nos aspectos eficazes presentes nessa estratégia PUIs, com o diferencial de aumentar a aderência das diretrizes estabelecidas. Quanto ao aumento da aderência das diretrizes estabelecidas, emprega-se PCAs sensíveis à atributos contextuais em filtros de acesso à Internet para aumentar a qualidade das regras de acesso. Entretanto, a tentativa de suprir os aspectos eficazes presentes das PUIs, diz respeito ao emprego das boas práticas dessa estratégia, como por exemplo a declaração de um acordo formal referente às instruções dos empregadores quanto a utilização da Internet no ambiente de trabalho.

Como visto no capítulo anterior, devido a alta dinamicidade da Internet, uma estratégia baseada em PCAs deveria ser atualizada constantemente. Dessa forma, quanto ao problema das PCAs tornarem-se obsoletas, utilizou-se o ciclo de melhoria contínua PDCA de modo que a criação de PCAs pudesse ser realizada através de etapas bem definidas, possibilitando uma ação reflexiva quanto as PCAs atuantes no filtro de acesso à Internet. Procurou-se basear esse ciclo na iteração entre as pessoas envolvidas na realização das tarefas. Dessa forma, pensou-se na necessidade de criar medidas para tornar interessante aos funcionários sua participação proativa quanto as melhorias no acesso à Internet. Portanto, integrou-se ao modelo, como medida de fomento, incentivos aos funcionários em caso de cumprimento das diretivas e em caso contrário a possibilidade da aplicação de medidas disciplinares. A Figura 4.1 ilustra o modelo.

No modelo, o ciclo de melhoramento contínuo está estruturado de acordo com o ciclo PDCA e compreende as etapas Planejar, Executar, Verificar e Agir. Na etapa **Planejar** a atividade *Brainstorming* tem como objetivo esclarecer os aspectos eficazes das PUIs e facilitar a elaboração de PCAs baseadas em atributos ao utilizar as informações da Estrutura Organizacional para extração de perfis. A utilização de diagramas PERT permite associar os recursos necessário da

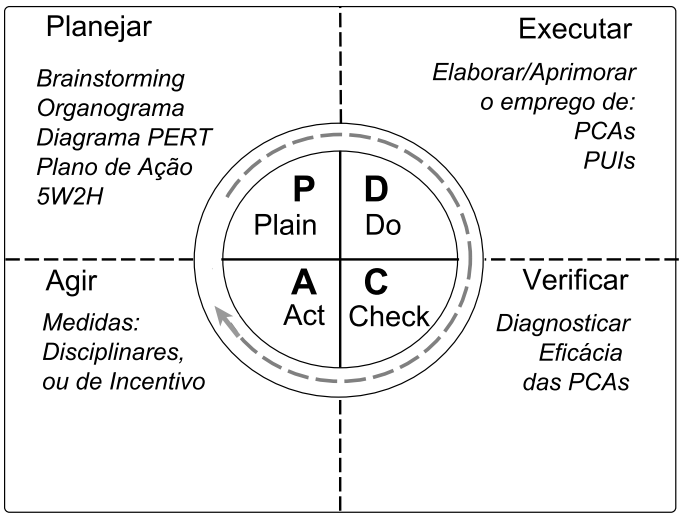


Figura 4.1: Modelo de Gestão para Prevenção da Má Utilização da Web

Web com as atividades que precisam ser desempenhadas na instituição. Enquanto que o Plano de Ação 5W2H associa os perfis extraídos com os recursos utilizados nas atividades, agregando ainda uma restrição temporal para que esta tarefa seja desempenhada. Dessa forma, extrai-se informações contextuais sobre como devem ser utilizados os recursos da *Web* conforme os interesses dos empregadores para serem aplicados nas PCAs baseadas em atributos.

Na etapa **Executar**, elaboram-se as PCAs baseadas em atributos com base na etapa de planejamento, aplicam-se tais PCAs no filtro de acesso e as diretrizes referente aos aspectos eficazes das PUI em contratos que devem ser assinados pelos funcionários. A etapa **Verificar** tem como objetivo acurar a eficácia da aplicação do modelo, utilizando técnicas de auditoria e monitoramento tais como acompanhamento por *logs*. Na etapa **Agir**, aplicam-se sistemas de gratificação onde se determinam as recompensas refentes ao bom cumprimento das normas estabelecidas pelos empregadores.

Para explicar mais detalhadamente os elementos do modelo, a seção 4.1 apresenta a etapa planejar, a seção 4.2 a etapa executar, na seção 4.3 a fase verificar, enquanto que na seção 4.4 o elemento agir.

4.1 Planejar

Nesta seção são detalhadas as atividades da etapa planejar do Modelo de Gestão para Prevenção da Má Utilização da *Web*. Como ilustrado no início do capítulo, mais precisamente na Figura 4.1, as atividades da etapa planejar consistem na utilização do *Brainstorming*, Organo-

gramas, Diagramas PERT e Plano de Ação 5W2H. Esta etapa abrange o problema da onerosidade na especificação das PCAs, o que torna essa atividade destinada à pessoas especializadas. Desse modo, esta seção explica como a elaboração e manutenção das PCAs pode ser realizada com base em conhecimentos administrativos. Todavia, considerando esse objetivo, além das atividades presentes na etapa planejar, torna-se necessário identificar como dá-se o processo de conversão dos dados contidos nas ferramentas administrativas do modelo para as PCAs que serão aplicadas nos filtros de acesso à Internet.

Portanto, para tornar claro e objetivo o desenvolvimento da seção considerou-se mais apropriado a criação de subseções explicando cada atividade da etapa de planejamento. Dessa forma, na seção 4.1.1 apresenta como se dá a utilização do *Brainstorming*, a seção 4.1.2 apresenta qual a função dos Organogramas, na seção 4.1.3 como se dá a utilização dos Diagramas PERT, a seção 4.1.4 demonstra qual o papel do Plano de Ação 5W2H no modelo, enquanto que a seção 4.2.0.1 demonstra como o modelo utiliza as informações contidas nas ferramentas administrativas para transpô-las para PCAs.

4.1.1 *Brainstorming*

O uso da ferramenta de *brainstorming* tem como objetivo esclarecer as diretrizes que estarão contidas nas PUIs e posteriormente nas PCAs, pois, pode-se dizer que uma das situações ideais para prática do *Brainstorming* é quando necessita-se de muitas idéias a respeito de determinado assunto (KOLFSCHOTEN, 2011). O uso dessa ferramenta administrativa é um meio de envolver os usuários e promover discussões de quais recursos da *Web* poderiam potencializar o desenvolvimento de suas atividades no trabalhos.

Todavia, percebe-se que nem sempre os usuários terão opiniões formadas em relação a como o uso dos recursos da Internet pode potenciar o desempenho da sua função. Pois, entende-se que para isto o usuário deve possuir um conhecimento considerável sobre os recursos da Internet para contribuir significativamente. Entretanto, em setores onde existe mão de obra mais especializada pode-se conseguir contribuições positivas em relação à esse assunto. De modo que sugere-se como uma boa prática que em setores onde percebe-se que os usuários não possuem conhecimento suficiente para contribuir, seja realizam selecionados representantes de grupos que apresentem a opinião da maioria.

Outra forma de aplicar *Brainstorming* é isolar os integrantes e entrevistá-los individualmente para evitar que os participantes se omitam e não expressem suas opiniões (DIEHL; STROEBE,

1987). Esta técnica é conhecida como *Brainstorming* Eletrônico e permite que os sujeitos entrevistados expressem suas opiniões sem revelar sua identidade, aumentando a eficiência desta ferramenta (POLLARD; CADSBY, 1996). Portanto, com o objetivo de evitar o bloqueio da iteração entre os integrantes da organização, o modelo proposto sugere a prática do *Brainstorming* Eletrônico.

4.1.2 Organogramas

Organogramas permitem obter de forma clara e rápida a hierarquia de perfis da organização, bem como estes se relacionam entre si. O modelo proposto utiliza organogramas para obter essas informações para as PCAs do modelo.

Para facilitar o entendimento de como essas informações podem ser retiradas do ambiente, vide o exemplo do indivíduo que desempenha na mesma instituição de ensino a função de programador de interfaces *Web* e aluno. Considerando este exemplo, a Figura 4.2 ilustra como os perfis envolvidos neste cenário se relacionam.

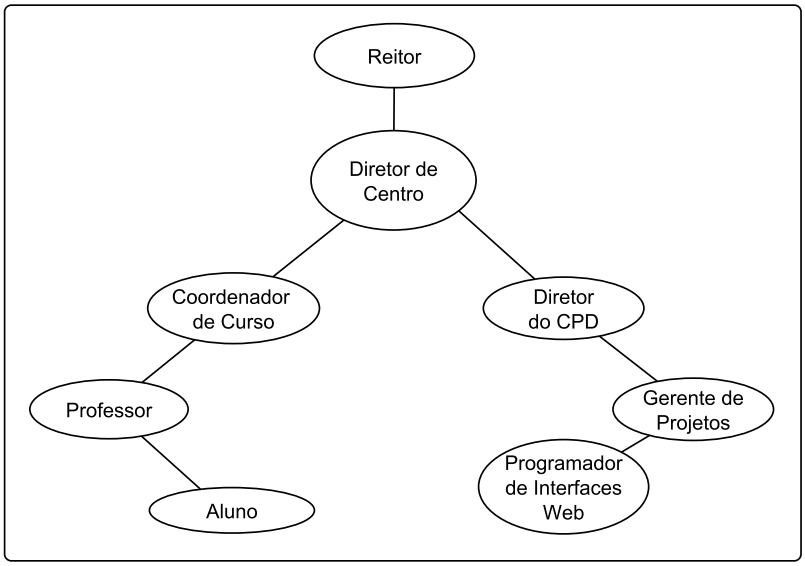


Figura 4.2: Exemplo de Organograma para o Ambiente Acadêmico

Na Figura 4.2 percebe-se que a autoridade máxima no ambiente acadêmico trata-se do reitor e que em ambas as situações, aluno ou servidor, o indivíduo do exemplo está sempre em níveis inferiores ao Diretor do Centro, ou seja, estará sempre sujeito a ele. Durante seu contrato de vinte horas como técnico administrativo alocado no CPD, que pertence ao centro de tecnologia, este indivíduo responde diretamente ao Gerente de Projetos e este possui como chefe direto o diretor do CPD, cujo chefe é o diretor do centro. Nos momentos que desempenha papel de

aluno, seu superior imediato é o professor da disciplina. Da mesma forma, o Professor está sujeito ao Coordenador de Curso.

Para enriquecer ainda mais este exemplo, suponha que o Gerente de Projetos utiliza o *Rational Unified Process* (RUP) (KRUCHTEN, 2003) como processo de desenvolvimento de *software*. Em sua metodologia, o RUP define perfis como representação de responsabilidades e comportamentos de um indivíduo ou grupo de indivíduos que trabalham em uma equipe, para demonstrar como estes se associam apresenta-se a Figura 4.3.

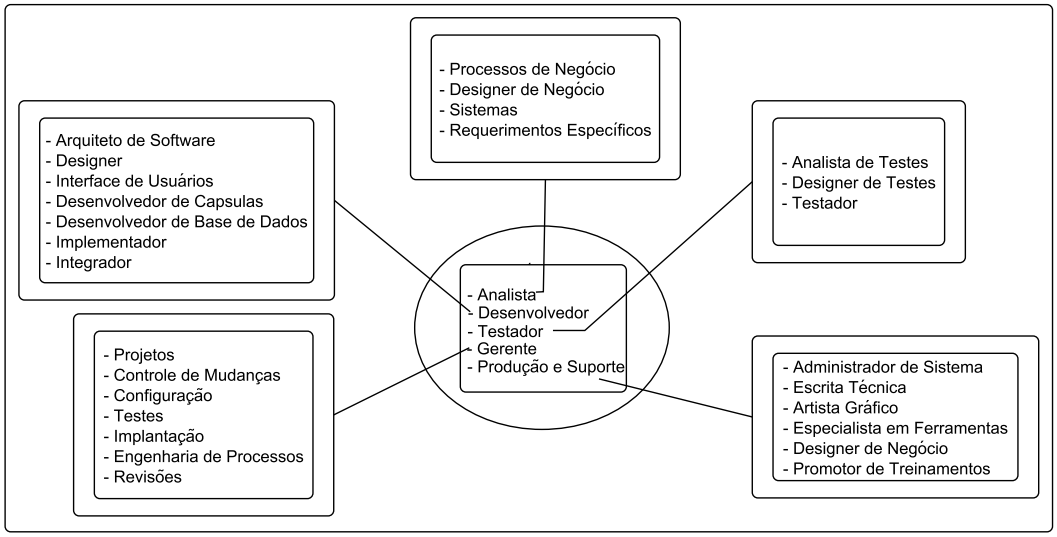


Figura 4.3: Exemplo de Organograma para o Desenvolvimento de um Projeto de Software. Adaptado de (KRUCHTEN, 2003)

Na Figura 4.3 nota-se que o papel de Analista no RUP agrega os papéis: Processos de Negócio, Designer de Negócio, Analista de Sistemas e Requerimentos Específicos. O perfil Desenvolvedor agrega os perfis: Arquiteto de Software, Designer, Interface de Usuários, Desenvolvedor de Capsulas, Desenvolvedor de Banco de Dados, Implementador e Integrador. O papel Testador incorpora os perfis: Analista de Testes, Designer de Testes e Testador. O papel de Gerente divide-se em Projetos, Controle de Mudanças, Configuração, Testes, Implantação, Engenharia de Processos e Revisões. Produção e Suporte agrega: Administrador de Sistemas, Escrita Técnica, Artista Gráfico, Especialista em Ferramentas, Designer de Negócio e Promotor de Treinamentos. Como pode-se observar, a utilização de organogramas ajudam na extração de perfis de forma rápida e clara.

4.1.3 Diagramas PERT

Esta seção demonstra como o uso dos Diagramas PERT auxilia o modelo na associação entre as atividades desempenhadas na organização e os possíveis recursos da Internet que potencializam sua realização. Retomando seu conceito, Diagramas PERT consistem em uma técnica para planejar atividades encadeadas, usadas em planejamentos, cronogramas e controle de projetos (DOUGLAS, 1978). Para exemplificar como esta técnica se aplica ao modelo proposto, consideremos o exemplo da seção anterior envolvendo um projeto de *software* que utiliza o processo de desenvolvimento de *software* RUP.

As atividades do RUP podem ser traduzidas em tarefas, essas tarefas podem ser representadas em um diagrama PERT. Considerando as fases do modelo RUP, pode-se dividir as atividades em diversas tarefas para conclusão de uma atividade. A Figura 4.4 ilustra esse conceito.

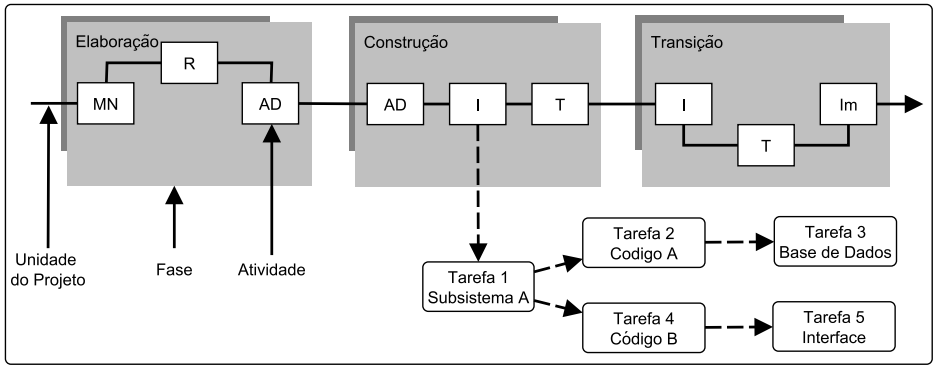


Figura 4.4: Exemplo de Diagrama PERT para o Gerenciamento de um Projeto de Software

Na Figura 4.4 pode-se observar na fase de Construção que a atividade de Implementação pode ser dividida em: Tarefa 1, Subsistema A, representando um fragmento do sistema a ser construído. Esse Subsistema é composto pelo desenvolvimento pela Tarefa 2, que constitui a criação do código A e consequentemente a tarefa 3, criação da Base de Dados. A tarefa 4, desenvolvimento do código B e Tarefa 5, desenvolvimento da Interface. Conforme o exemplo, a utilização desta ferramenta administrativa permite ao modelo associar os recursos disponíveis na Internet com as tarefas que o gestor julge necessárias.

4.1.4 Plano de Ação 5W2H

No modelo, o objetivo do Plano de Ação 5W2H é absorver os elementos Organograma e Diagramas PERT no mapeamento de atividades, adicionando restrições temporais, considerando a hierarquia de papéis apresentados na Seção 4.1.2 e o fluxo de tarefas da Seção 4.1.3, em

conjunto com a necessidade de estabelecer restrições temporais para cada iteração do projeto. Desse modo, o Plano de Ação pode relacionar os papéis definidos para a equipe de desenvolvimento com o fluxo de tarefas dos diagramas PERT e definir qual conjunto de recursos da Web são necessários para execução das tarefas em conjunto com o cronograma definido pelo gerente de projetos. A Tabela 4.1 demonstra como o plano de ação agrega essas definições.

Tabela 4.1: Plano de Ação 5W2H para o Gerenciamento de Projeto de Software

Planilha 5W1H		Projeto:											
O QUÊ		**POR QUÊ**	**QUEM**	**COMO**				**CRONOGRAMA 2011**					
item				item	Quem	Necessidade de Acesso	Data Limite	Janeiro à Junho					
1	T2	SA	Analista de Sistemas	1.1	Ricardo	Mensagens Instantâneas	28/02/2011	X	X				
2	T3	T2	Desenvolvedor BD	2.1	Pedro	Wikis	28/02/2011	X	X				
3	T4	SA	Implementador	3.1	Paulo	Blogs sobre Java	30/04/2011			X	X		
4	T5	T4	Interface de Usuário	4.1	Mateus	Facebook	30/04/2011			X	X		

Observe que a Tabela 4.1 representa as informações contextuais apresentada anteriormente em linguagem de alto nível de abstração através das ferramentas administrativas que compõem o modelo proposto na seção 4.

4.2 Executar

O objetivo da etapa Executar é a elaboração e manutenção de PCAs e PUIs conforme as necessidades encontradas quanto ao planejamento.

Como visto no Capítulo 2, os critérios considerados eficazes das PUIs são classificados entre a clareza na definição dos deveres dos empregados e dos direitos dos empregadores. Além disso, vale lembrar que o conceito de PUIs está relacionado com a definição de diretrizes quanto ao uso dos recursos tecnológicos no trabalho. De forma que em possíveis ocorrências criminais que envolva os recursos tecnológicos do empregador, torna-se interessante possuir uma prova legal do reconhecimento dos funcionários quanto as diretrizes definidas. Desse modo, as atividades da etapa Executar consistem no emprego dos critérios eficazes das PUIs e das PCAs na construção dos filtros de acesso à Internet.

Portanto, o emprego dos critérios eficazes das PUIs nesta etapa diz respeito à aplicação de um contrato formal, especificando diretrizes estabelecidas pelos empregadores. Percebe-se que o modelo não é rígido quanto a forma como se emprega esse contrato. De modo que este pode ser aplicado como um contrato padrão, ou *on-line* através de certificados e assinaturas digitais. Enquanto que a aplicação das PCAs em filtros de acesso, consiste na alimentação da

base de dados onde o filtro de acesso realiza busca à procura de PCAs. Note que o modelo não determina a forma de armazenamento das políticas ou critérios de otimização de buscas.

4.2.0.1 Transposição das Informações para PCAs

Esta Seção demonstra como resultado a política gerada pela utilização do modelo proposto. A Política 4.1 apresenta a política gerada com base no plano de ação apresentado anteriormente.

```
1  Acessar(u, s, a) ←
2   (Perfil(u) = 'Analista de Sistemas'
3    ∧
4   Classificacao(s) ϵ {'Mensagens Instantaneas'}
5    ∧
6   (Tempo(a) ≥ 01/01/2011 ∨ Tempo(a) ≤ 28/02/2011))
7
8   ∨
9
10  (Perfil(u) = 'Desenvolvedor BD'
11   ∧
12  Classificacao(s) ϵ {'Wikis'}
13   ∧
14  (Tempo(a) ≥ 01/01/2011 ∨ Tempo(a) ≤ 28/02/2011))
15
16  ∨
17
18  (Perfil(u) = 'Implementador'
19   ∧
20  Classificacao(s) ϵ {'Blogs sobre Java'}
21   ∧
22  (Tempo(a) ≥ 01/03/2011 ∨ Tempo(a) ≤ 30/04/2011))
23
24  ∨
25
26  (Perfil(u) = 'Desenvolvedor de Interface Web'
27   ∧
28  Classificacao(s) ϵ {'Redes Sociais'}
29   ∧
30  (Tempo(a) ≥ 01/03/2011 ∨ Tempo(a) ≤ 30/04/2011))
```

Política 4.1: Política Gerada pelo Modelo de Gestão para Prevenção do Risco da Má Utilização da Web

Como pode-se observar na Política 4.1, as linhas representam as definições apresentadas anteriormente no plano de ação da Tabela 4.1. A primeira regra define que o Analista de Sistema tem permissões para Mensagens Instantaneas no período de 01/01/2011 até 28/02/2011 (mês de Janeiro e Fevereiro). Na regra seguinte, o Desenvolvedor BD tem acesso aos *Wikis* no período que vai de 01/01/2011 até 28/02/2011. A seguir, o Implementador pode interagir com Blogs sobre Java e tem permissão de 01/03/2011 até 30/04/2011 (Março à Abril). A última regra, diz que Interface Usuario tem permissões para Redes Sociais no período de 01/03/2011 até 30/04/2011.

As regras que definem a política são implementadas em uma linguagem de alto nível de acordo com os elementos contextuais. Isto é, as regras são definidas de acordo com: quem terá

acesso, a qual tipo de elementos e por um período de tempo. Desta forma, a complexidade de implementação do mapeamento dos atributos referentes ao contexto é diminuida, facilitando a implementação por usuários que não possuem conhecimentos técnicos nesta área.

4.3 Verificar

A etapa Verificar objetiva acurar a aplicabilidade das decisões tomadas na etapa Planejar e empregadas na etapa Executar. Dessa forma, o modelo é flexível quanto a forma que se determinará à acurácia das decisões empregadas, sugerindo para esta etapa o monitoramento de indicadores de aderência, ou seja, o acompanhamento de possíveis pistas de má utilização da *Web*. Dentre essas pistas, pode-se citar o monitoramento de *logs* de acesso à Internet e gráficos de gerenciamento da utilização da Internet.

A capacidade de tráfego de informações que a organização contrata junto a um provedor de serviços de Internet e a utilizada pode ser monitorada por gráficos de gerenciamento da utilização dessa banda obtidos através da utilização de ferramentas de gerenciamento de redes.

Essa etapa possui uma importância muito significativa, visto que os dados coletados nela servem de parâmetro para próxima fase do modelo, pois a criação de indicadores relevantes e maduros são de fundamental importância para o sucesso na implementação do modelo.

4.4 Agir

A etapa Agir consiste no emprego de medidas de incentivo para os usuários que cumprirem as diretrizes e em contrapartida, para os descumpridores a aplicação de medidas disciplinares. Esta etapa está relacionada com o envolvimento da alta gerência, pois o emprego das medidas de incentivo e disciplinares estão diretamente relacionadas com investimentos em segurança e gestão de pessoas, respectivamente. Considera-se interessante a criação de um sistema de gratificação que condicione os usuários a cumprir as normas de segurança, promovendo a cultura da segurança preventiva a má utilização da Internet no ambiente de trabalho.

Nesta etapa pode-se criar diferentes níveis de recompensa para aumentar o envolvimento dos colaboradores. Por exemplo, o fato do envolvimento de usuários, ou seus representantes, no planejamento já constitui em uma espécie de recompensa, pois tais pessoas passam a se considerar coautoras das diretrizes estabelecidas, uma vez que já participaram da elaboração das políticas. Outro exemplo simples que pode ser utilizado no sistema de gratificação trata-se da classificação dos usuários identificados como cumpridores das diretrizes e sua posterior

divulgação como usuário modelo.

Todavia, considerando casos de detecção da má utilização da Internet, torna-se necessária a aplicação de medidas disciplinares. Sendo que o nível das medidas empregadas varia conforme a gravidade do comportamento abusivo. Por exemplo, um caso onde um aluno adquire material protegido por direitos autorais através da Internet e a universidade passa a responder juridicamente por essa atitude, pode ser tratado com mais rigor do que se este aluno obteve acesso à transmissão de música através rádios na Internet. Entretanto, considerando que este estivesse armazenando e disseminando material de pornografia através de servidores internos da universidade, medidas disciplinares mais impactantes podem ser tomadas.

Observa-se que para prover a melhoria contínua, esta etapa do modelo proposto emprega duas abordagens: medidas disciplinares e de incentivo. As de incentivo objetivam condicionar os usuários a não utilizar de maneira incorreta a Internet, ou seja, prevenir o comportamento indesejado, enquanto que as medidas disciplinares visam aplicar métodos para corrigir o comportamento inadequado em relação à Internet através de punições que devem estar esclarecidas na PUI empregada na fase Executar. As infrações detectadas devem ser devidamente documentadas nesta etapa para que na próxima iteração do ciclo PDCA elas sejam consideradas na etapa Planejar.

4.5 Considerações Finais

Este capítulo apresentou o Modelo de Gestão para Prevenção da Má Utilização da *Web*, cujo objetivo consiste em prover o processo de gerenciamento de PCAs com granularidade fina através de um ciclo de melhoria contínua. Observou-se que para realizar este objetivo constituiu-se o modelo com base no ciclo de melhoria contínua PDCA, onde adicionaram-se atividades específicas em suas respectivas etapas: Planejar, Executar, Verificar e Agir.

A etapa Planejar do modelo possuiu a incumbência de gerenciar PCAs com base em ferramentas administrativas. Para isto, agregou-se à etapa Planejar as atividades: *Brainstorming*, Organogramas, Diagramas PERT e Plano de Ação 5W2H, onde a atividade de *Brainstorming* extrai dos usuários possíveis recursos da Internet que potencializem a realização de suas funções, o emprego de Organogramas possibilita estabelecer a hierarquia de funções da organização, os Diagramas PERT possibilitam a definição das tarefas provenientes de cada perfil em conjunto com dados contextuais referente a quando as tarefas devem ser desempenhadas, o Plano de Ação 5W2H agrega todas as informações definidas nas ferramentas anteriores para

deixá-las mais enxutas, salientando as restrições temporais para cada perfil. Dessa forma, a etapa planejar possibilita a transposição simplificada das informações contidas em cada ferramenta administrativa para as PCAs, facilitando o processo de elaboração e manutenção das PCAs por pessoas sem conhecimentos técnicos específicos.

Na etapa Executar, além da elaboração e manutenção das PCAs, incluiu-se as atividades referente a aplicação das PCAs em filtros de acesso à Internet e os critérios eficazes das PUIs em diretrizes empresariais. Desta forma, esta etapa viabiliza a revisão periódica (a cada ciclo do modelo) da PUI, das PCAs, dos filtros de acesso e das diretrizes da empresa.

Na etapa Verificar, sugeriram-se a utilização de indicadores para acurar a eficácia da gestão empregada pelo modelo, servindo como parâmetro para a etapa seguinte. Visto que a etapa Agir agrega elementos responsáveis por aplicar medidas disciplinares ou de incentivo. Salienta-se que o parâmetros utilizados para aplicar tais medidas são extraídos da atividade Verificar.

A iteração periódica do ciclo de melhoria promove uma gestão sistêmica que permite prevenir a má utilização da *Web* em ambientes empresariais.

5 SISTEMA DE GESTÃO DE POLÍTICAS DE CONTROLE DE ACESSO

Esse capítulo descreve detalhes da implementação do *software* do Sistema de Gestão de Políticas de Controle de Acesso (SGPCA). Como visto no capítulo 3, o problema do emprego de PCAs sensíveis à atributos contextuais na gestão da má utilização da *Web* consiste na onerosidade do processo de elaboração, que normalmente requer conhecimento técnico específico. Para suprir essa carência, o SGPCA tem como objetivo servir como uma interface amigável para criação de PCAs. A Seção 5.1 descreve as características gerais da ferramenta, na Seção 5.2 se descreve como é realizada a geração de PCAs, enquanto a Seção 5.2.1 apresenta um estudo comparativo entre o SGPCA e os *softwares* atualmente utilizados na gestão de acessos à Internet. Ao final são apresentadas as conclusões parciais do capítulo (Seção 5.3).

5.1 Características da Ferramenta

O processo de elaboração e manutenção de PCAs pode se tornar complexo, ou pelo menos especializado, devido o alto nível de expertise técnica envolvida, dado que para desempenhar tal tarefa torna-se necessário o conhecimento de linguagens de especificação de PCAs tais como a *eXtensible Access Control Markup Language* (XACML). Além disso, em organizações onde o número de usuários internos é expressivo esse processo pode ser ainda mais despendioso. Dessa forma, o objetivo da ferramenta desenvolvida é auxiliar a aplicação do modelo proposto no Capítulo 4, de modo que os gestores sem a expertise em linguagem específicas possam realizar o gerenciamento de PCAs.

Prevista para ser uma aplicação *Web*, que possibilita acesso de qualquer local, o desenvolvimento do *software* SGPCA utilizou a linguagem de programação *Personal Home Page*: *Hypertext Preprocessor* (PHP) [1], banco de dados *MySQL* [2], linguagem de especificação de políticas de controle de acesso XACML [3], a biblioteca *NuSOAP* [4] e as classificações de sites da base *Shallalist* [5].

No protótipo desenvolvido, para a geração de PCAs foram utilizados seis objetos, sendo eles: Professor, Disciplina, Dia da Semana, Tipos de Navegação, Sistema Gerenciador de Base

[1] http://php.net/
[2] http://www.mysql.com/
[3] http://www.oasis-open.org/committees/xacml/
[4] http://sourceforge.net/projects/nusoap/
[5] http://www.shallalist.de/categories.html

de Dados (SGBD) e Sistema de Arquivos, conforme ilustra o diagrama de caso de uso da Figura 5.1.

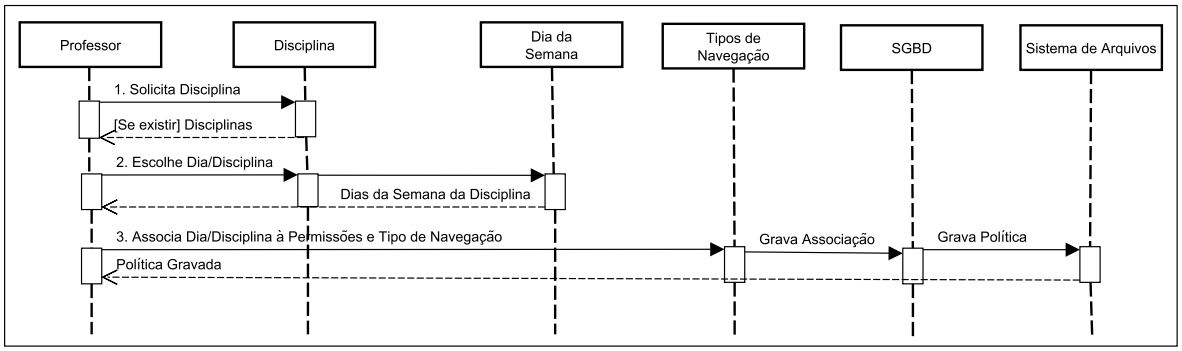


Figura 5.1: Diagrama de Sequência para Criação de uma PCA

A iteração entre os objetos aponta a sequência de eventos realizados quando um professor cria uma política de controle de acesso para sua disciplina. O professor deve primeiro solicitar uma disciplina, escolher o dia de ocorrência das aulas que pretende controlar o acesso, bem como associar o par Dia/Disciplina às permissões e Tipos de Navegação pretendidas. Após a troca de mensagens e armazenamento no SGBD das opções escolhidas pelo professor o SGPCA, de posse destes dados, codifica a PCA em formato XACML e a armazena no sistema de arquivos. A escolha de utilizar o SGBD, ao invés de apenas o sistema de arquivos, deu-se pelo fato que o SGBD apresenta maior flexibilidade na manipulação dos dados. Desta forma, possibilita-se possíveis manutenções na PCA e somente após o armazenamento das associações dos objetos no SGBD, o SGPCA gera a PCA que será de fato aplicada.

O modelo entidade relacionamento, apresentado na Figura 5.2, foi elaborado para dar suporte à geração de PCAs para do SGPCA. Cada professor pode ter inúmeras turmas, sendo que cada turma também pode ter inúmeros professores. As turmas são compostas pela união de um curso e uma disciplina e deve estar relacionada com o horário, que trata-se da entidade responsável por agregar o dia da semana, tipo de aula (teórica ou prática), intervalo (entre períodos ou no final da aula) e horário de início e término. Dessa forma a base de dados pode armazenar as características temporais sobre as disciplinas.

No diagrama (Figura 5.2) existe uma associação de muitos para muitos entre horários e classificação, de modo que a entidade classificação possa ser responsável por armazenar os tipos de navegação que os professores poderão gerir, contando ainda com o atributo descrição, cujo objetivo é informar detalhes sobre o tipo de navegação.

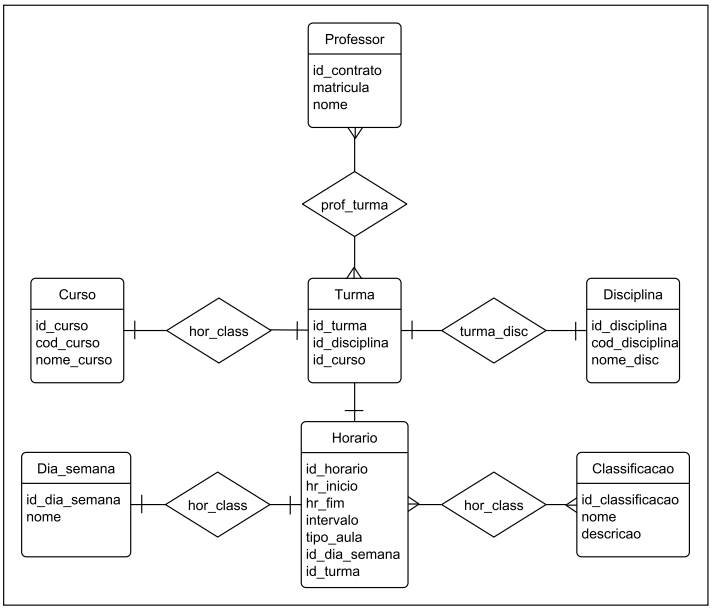


Figura 5.2: Modelo Entidade Relacionamento do SGPCA

Em síntese, a ferramenta SGPCA oferece uma interface amigável ao gestor de políticas de controle de acesso, deixando transparente para o usuário o processo de geração e armazenamento das PCAs em XACML.

5.2 Geração de Políticas de Controle de Acesso

Após a autenticação no sistema, o professor deve selecionar a disciplina do curso desejado para elaboração ou manutenção da PCA, sendo o passo inicial para o processo de gerenciamento. A Figura 5.3 ilustra a escolha da disciplina, que baseia-se tanto no nome da disciplina quanto seu respectivo código. Optou-se por essa nomenclatura devida as peculiaridades da instituição de ensino na qual se aplicou o sistema. Considerando a seleção da disciplina de Laboratório de Programação II, a Figura 5.4 apresenta a escolha do dia da semana.

Pode-se perceber que na Figura 5.4 além do dia da semana, apresenta-se também o horário e o tipo de aula que é ministrada, teórica ou prática. Essa flexibilidade permite aos professores criar políticas específicas para aulas teóricas ou práticas. Dessa forma, devido essas particularidades pode-se ter uma aula com dois períodos, cada período com tipos de aulas diferentes e em cada tipo de aula os alunos podem ter acessos diferentes, conforme as necessidades do professor.

Após a escolha da disciplina, em conjunto com seu possível tipo de aula, o professor tem a opção de associar os tipos de navegação para a disciplina, horário e tipo de aula selecionado.

Figura 5.3: Tela para Escolha da Disciplina que se Aplicará a PCA

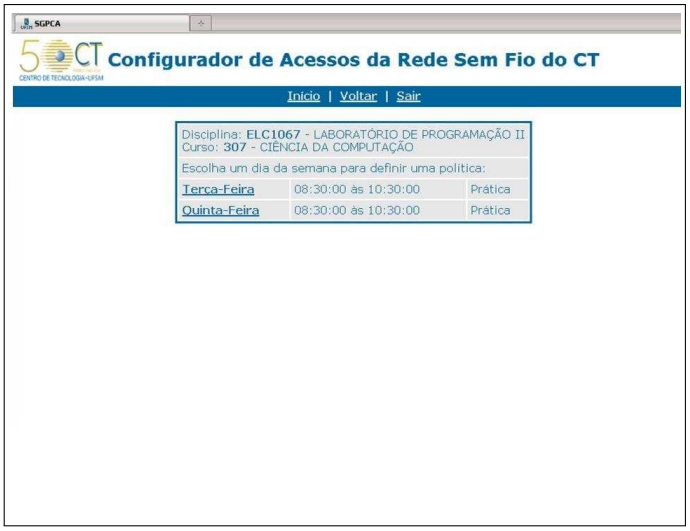


Figura 5.4: Tela com Opções de Dias da Semana em que a PCA Entrará em Vigor

Para os tipos de navegação, selecionou-se nove classificações da base *Shallalist* [6], as que foram consideradas mais relevantes por relacionar-se com os tipos de navegações que em alguns momentos poderiam ser uteis para algumas disciplinas e em outros momentos poderiam ser classificados como má utilização da Internet. A Figura 5.5 ilustra essa associação. Optou-se pelo uso de tipos de navegação para evitar que os professores cadastrem as URLs que desejam ou não ter acesso, o que tornava complexo a manutenção das políticas. Desse modo, basta o professor selecionar o tipo de navegação desejada que os dados referente às URLs do tipo selecionado são importados da base *Shallalist*. Para permitir um tipo de site o professor deve selecionar a opção *Permitir*, caso contrário a opção *Negar*. Cabe salientar que essas opções são mutuamente exclusivas, ou seja, pode-se selecionar apenas *Permitir* ou *Negar*.

[6] http://www.shallalist.de/categories.html

Figura 5.5: Tela de Configuração das Permissões e Horários

Tendo realizada a associação entre permissões e tipos de navegação, o processo de elaboração ou manutenção da PCA é finalizado, de modo que o professor recebe a mensagem de política gravada com sucesso, conforme ilustrado na Figura 5.6

Figura 5.6: Tela de Confirmação da Criação de PCA

Após essa sequência de passos, o SGPCA alimenta a base de dados MySQL gera a PCA no formato XACML, gravando-a no sistema de arquivos, conforme o diagrama de sequência ilustrado na Figura 5.1.

5.2.1 Estudo Comparativo

Esta seção apresenta um estudo comparativo entre o SGPCA e os *softwares MyHotSpot* [7], *Mikrotik* [8] e *Squid* [9] que são atualmente utilizados na gestão de acessos à Internet. O objetivo desta comparação consistiu em demonstrar que o SGPCA emprega PCAs com granularidade mais fina que as soluções existentes, possibilitando um método de autenticação flexível, não exigindo conhecimento específico de administração de redes à baixo custo de aquisição. Para isto, as características utilizadas na comparação consistiram no tipo de PCA, método de autenticação, a necessidade de conhecimento técnico para administração e o tipo do *software*. A Tabela 5.1 apresenta essa comparação.

Tabela 5.1: Comparativo Entre o SGPCA e *Softwares* Atualmente Utilizados

Proxy	Tipo de PCA	Autenticação	Administração Exige Conhecimento Técnico	Tipo
MyHotSpot	-	Sistema Operacional	Não	Livre
Mikrotik	DAC	RADIUS	Sim	Comercial
Squid	DAC/RBAC	LDAP, Samba e RADIUS	Sim	Livre
SGPCA	Baseada em atributos	*Web Service*	Não	Livre

Na Tabela 5.1 percebe-se que as características fortes do *MyHotSpot* consistem na não exigência de conhecimento técnico para o gereciamento e por este ser distribuído gratuitamente, apesar de não possuir seu código aberto. Nota-se que esta ferramenta não apresenta nenhum tipo de PCA, pois apresenta a possibilidade de bloqueio individual de usuários. Esse bloqueio pode ocorrer em dois momentos, quando o administrador julgar necessário ou quando acabarem os créditos de navegação do usuário. Observa-se ainda que este *software* utiliza a autenticação do sistema operacional, fato que elimina o processo de autenticação via rede e agiliza o acesso à Internet. No entanto, torna necessário a instalação de um aplicativo nos dispositivos de acesso que se comunica com o servidor informando o nome do usuário e do computador que está acessando a rede.

O *Mikrotik* apresenta como pontos positivos o fato deste ser largamente utilizado no Brasil, a utilização de um tipo de PCA e a autenticação através do *Remote Authentication Dial In User Service* (RADIUS) [10], que agrega maior confiabilidade no processo de autenticação e pode ser integrado com outros sistemas computacionais. No entanto, como o tipo de PCA adotado por

[7] http://www.mypublicwifi.com/myhotspot/en/index.html
[8] http://www.mikrotik.com/
[9] http://www.squid-cache.org/
[10] http://freeradius.org/

essa ferramenta consiste nas DAC, a granularidade destas PCAs é grossa. Apesar deste *software* ser comercial, o custo de sua licença é considerado baixo, o que em conjunto com sua qualidade facilitou sua larga disseminação.

Em relação ao *Squid*, os motivos que levaram a sua escolha trataram-se do fato deste empregar PCAs DAC, RBAC e diversas formas de autenticação. Esta solução livre de código aberto possibilita a utilização de perfis, através da criação de grupos de usuários, listas gravadas em sistema de arquivos, onde cada grupo é associado com um arquivo que contém os acessos permitidos, o que exige conhecimento de administração de servidores. Vale ressaltar que apesar desta possibilidade, percebe-se que a maioria dos administradores utilizam políticas DAC, o que gera um controle de acesso menos flexível. Nota-se ainda que dentre os métodos de autenticação do *Squid* possibilita a utilização do *Lightweight Directory Access Protocol* (LDAP) [11], Samba [12] e RADIUS.

Percebe-se que quanto ao tipo de PCA, o SGPCA apresenta PCAs baseadas em atributos contextuais, ou seja, com granularidade fina, permitindo criar regras mais flexíveis e dinâmicas que os demais. Quanto ao método autenticação, o *software* proposto emprega a tecnologia *Web Service* que possibilita, assim como o RADIUS e o LDAP, utilizar as credenciais de outros sistemas da empresa para autenticação na rede. Além disso, assim como o *MyHotSpot*, o SGPCA não exige conhecimento de rede para gestão das PCAs que regularão o acesso à Internet, com adição de ser uma solução livre.

5.3 Considerações Finais

Neste capítulo foi descrito o Sistema de Gestão de Políticas de controle de Acesso, seu diagrama de sequência, modelo de dados e funcionalidades.

Tal sistema foi projetado para auxiliar a implantação do Modelo de Gestão de Prevenção da Má Utilização da Web. Mais precisamente, o sistema facilita o processo de elaboração e manutenção de políticas de controle de acesso pertencentes a etapa Executar.

Com o auxílio de uma ferramenta automatizada o processo de elaboração e manutenção de PCAs torna-se mais simples e menos oneroso para a organização, facilitando o gerenciamento de acesso e reduzindo os custos. Apresentou-se também um estudo comparativo do SGPCA com os *softwares MyHotSpot*, *Mikrotik* e *Squid*, onde demonstrou-se que o *software* proposto emprega PCAs com granularidade mais fina que os demais, possui um método de autenticação

[11] http://www.openldap.org/
[12] http://www.samba.org/

integrável com outros possíveis sistemas das instituições e não exige conhecimento de gerência de rede para criação das PCAs, tendo ainda a vantagem de ser uma solução livre.

6 ESTUDO DE CASO

Este capítulo apresenta o estudo de caso onde se aplicou uma iteração do modelo para gestão da rede sem fio de uma empresa pública, cuja atividade fim trata-se do ensino superior. O objetivo deste estudo consistiu em avaliar a aplicabilidade do modelo na gestão da má utilização da *Web* através de um ciclo de melhoria contínua. Para melhor apresentar este estudo, a Seção 6.1 descreve detalhes referentes ao ambiente de testes. Em seguida, na Seção 6.2, demonstra-se mais precisamente como a aplicação do modelo, em conjunto com o *software* SGPCA, proporcionou às pessoas sem conhecimentos técnicos específicos, neste caso professores, gerir PCAs com granularidade fina. Enquanto que na Seção 6.3 apresentam-se as considerações finais desse capítulo.

6.1 Ambiente de Testes

O ambiente onde aplicou-se o estudo de caso contou-se com 297 pessoas (33 professores e 264 alunos), pertencentes aos cursos de graduação em Ciência da Computação e Sistemas da Informação da Universidade Federal de Santa Maria (UFSM), compreendendo o período de 1 de Setembro à 11 de Dezembro de 2011.

Para tornar possível a gestão de acessos a nível de rede modificou-se o servidor *proxy Squid*, onde alterou-se o código fonte do módulo *rewrite*. Para que, quando realizadas, as solicitações de acesso à Internet primeiramente os usuários fossem redirecionados à uma página de autenticação. Tendo realizada a autenticação, as autorizações de acesso dos alunos passassem a ser realizadas pelo Serviço *Web* apresentado em (MACEDO; MOZZAQUATRO; NUNES, 2010).

A função deste serviço consiste em interpretar PCAs sensíveis à atributos contextuais, tornando este o mecanismo responsável por autorizar ou proibir o acesso aos sites requisitados. Para prover este serviço, o mecanismo referido cria uma requisição interna, codificada em XACML, contendo os atributos contextuais do requisitante, provenientes do sistema acadêmico, para então confrontá-la com as PCAs estabelecidas.

Para análise do tráfego de rede, foi utilizada a ferramenta *n-top* [1]. Enquanto que escolheu-se a rede *Wireless* do Centro de Tecnologia, pertencente à instituição de ensino, como recurso computacional a ser gerenciado. Escolheu-se a rede sem fio pois a mesma era liberada apenas para os professores e os mesmos possuíam receio em permitir o acesso aos alunos.

[1] http://www.ntop.org

Utilizou-se como repositório de atributos contextuais as informações presentes no sistema acadêmico da universidade. Dentre as informações deste sistema, foram utilizadas as disciplinas cursadas pelos alunos, horários de início e término das aulas e as matrículas dos docentes responsáveis pelas disciplinas. Com a agregação destes dados ao SGPCA, tornou-se possível aos professores elaborar e gerenciar PCAs aplicáveis somente as suas aulas.

Para facilitar tanto o entendimento desse processo, quanto o entrosamento entre os recursos humanos e computacionais, a Figura 6.1 ilustra a sequência de passos de uma autorização de acesso.

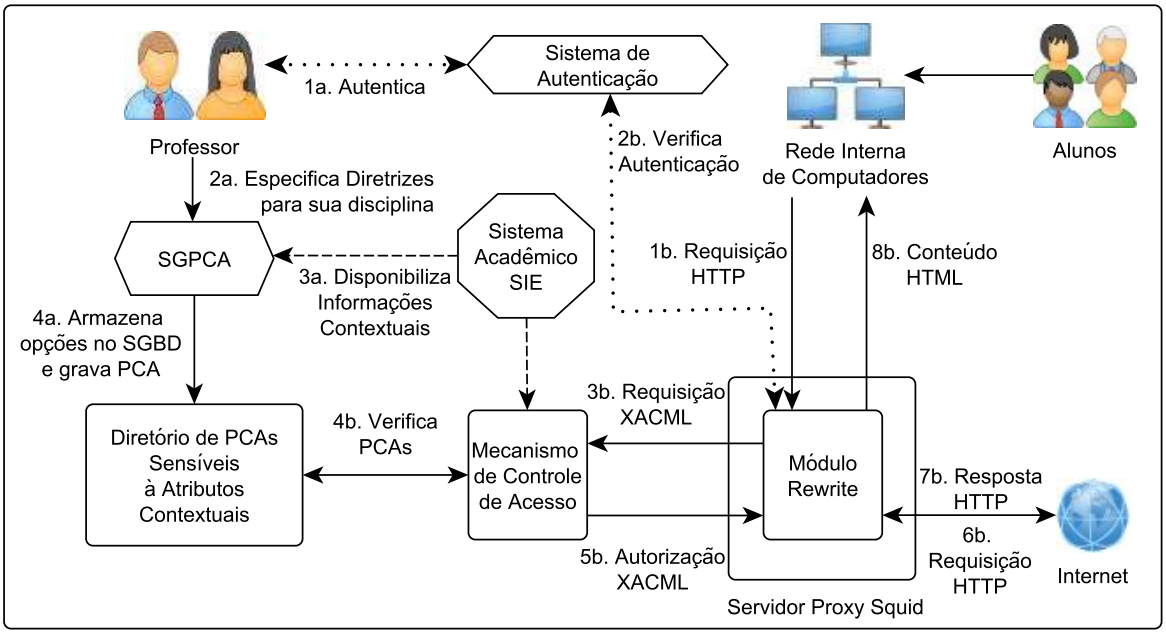


Figura 6.1: Passos para Solicitação e Concessão de Acesso no Ambiente de Testes

Na Figura 6.1 os números dos passos referentes a solicitação de acesso estão acompanhados da letra *a*, enquanto que os da concessão, acompanham a letra *b*. Referente a concessão de acesso, sempre que o professor achar necessário, ao acessar o SGPCA primeiramente o sistema solicita uma autenticação deste professor, requisitando as mesmas credenciais dos demais sistemas utilizados na universidade (passo 1a). Após a autenticação ser realizada com sucesso, o professor especifica as diretrizes de acesso para sua(s) disciplina(s) (passo 2a) que conta com os dados acadêmicos as disciplinas, tais como horários de início e fim, dia da semana e alunos matriculados providos pelo sistema acadêmico SIE (passo 3a). Tendo especificado as diretrizes, o SGPCA armazena estas opções no SGBD e armazena a PCA em sistema de arquivos (passo 4a).

Considerando a solicitação de acesso, um usuário ao tentar acessar a Internet dispara uma requisição *Hypertext Transfer Protocol* (HTTP) para à Internet (passo 1b). Nesse instante o servidor *Proxy Squid* intercepta esta requisição HTTP e verifica se este indivíduo realizou uma autenticação de acesso (passo 2b), tal verificação é realizada pelo módulo *rewrite*. Considerando que o sujeito foi devidamente autenticado, o módulo *rewrite* envia uma Requisição XACML para o mecanismo de controle de acesso a fim de obter uma autorização (passo 3b).

Este, por sua vez, monta uma Requisição XACML, contendo atributos contextuais extraídos do sistema acadêmico e analisa as PCAs sensíveis à atributos contextuais (passo 4b). Os atributos contextuais utilizados trataram-se das disciplinas que cada aluno está matriculado, horário de início e fim e o docente de cada disciplina. Para extração de tais informações, desenvolveu-se um aplicativo que exportava as informações da base de dados da UFSM para o banco de dados do mecanismo de controle de acesso.

Após percorrer as PCAs, confrontando-as com a Requisição XACML, o mecanismo de controle de acesso obtém uma autorização de acesso XACML e a encaminha ao módulo *rewrite* (passo 5b). Supondo que o mecanismo de controle de acesso autorize o indivíduo, dessa forma a requisição HTTP é permitida para a Internet (passo 6b) e o Servidor *Proxy* realiza o *download* do seu conteúdo (passo 7b), que finalmente é enviado ao navegador do usuário (passo 8b). Caso de um indivíduo receba uma negação de acesso, o servidor *Proxy* envia o conteúdo HTML de uma página informando que o acesso não foi autorizado.

Ao ocorrer uma situação onde um usuário não consiga se autenticar, o sistema entra em *loop*, entre o passo 1 e 8b, pedindo uma credencial válida, porém na terceira falha de autenticação a conta do usuário fica temporariamente bloqueada por 12 horas. Tendo descrito o ambiente de testes, pode-se agora demonstrar como se deu a aplicação do modelo.

6.2 Aplicação do Modelo

Esta seção demonstra a aplicação de um ciclo do modelo proposto na gestão da má utilização da *Web* em um ambiente real. Para se ter uma métrica da eficácia do modelo, tornou-se necessário realizar uma pré coleta de dados para servir como parâmetro na etapa *Verificar*. Desse modo, a Seção 6.2.1 apresenta a pré coleta dados coletados. Na Seção 6.2.2 apresenta-se a etapa *Planejar*, onde professores definiram diretrizes para compor a. A Seção 6.2.3, apresenta a etapa *Executar*, explicando como aplicou-se PCAs e PUIs. Na Seção 6.2.4, apresenta-se a análise realizada na etapa *Verificar*. Enquanto que na Seção 6.2.5 apresenta-se a etapa *Agir*.

6.2.1 Pré Coleta de Dados

Nesta seção apresentam-se os resultados da Pré Coleta de Dados. O objetivo dessa atividade, consistiu em se obter uma amostra de como se dava o acesso à Internet no Centro de Tecnologia da UFSM antes da aplicação do modelo. Deste modo, realizou-se uma coleta de tráfego totalizando 13 semanas, durante o período de 01 de Setembro à 27 de Novembro de 2011.

A coleta tornou possível identificar quais os tipos de navegação eram mais utilizados. Vale ressaltar que durante o período de análise, o acesso à rede sem fio foi permitido somente aos servidores da instituição. Para que fosse possível contabilizar o número de acessos aos tipos de navegação mais utilizados, utilizou-se uma ferramenta de monitoramento desenvolvida no grupo de pesquisa, visto que a mesma possibilita a geração de relatórios de acordo com as disciplinas cursadas. A Figura 6.2 ilustra quais sites foram os mais acessados nesse período.

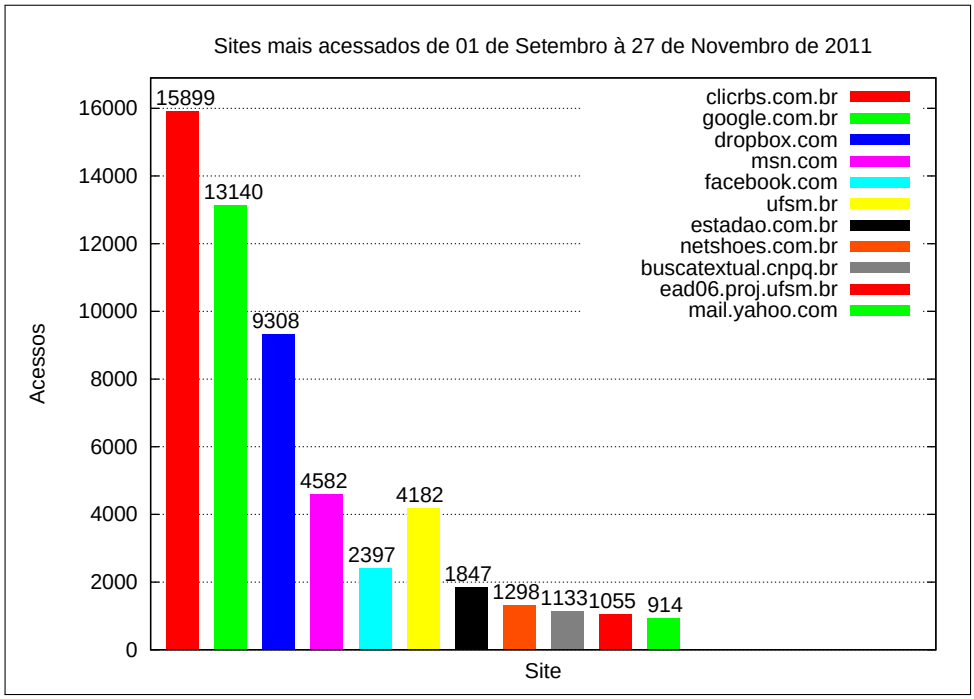


Figura 6.2: Coleta de Acessos Web Pré Implantação

Na Figura 6.2, pode se notar que durante o período da pré coleta, o site mais acessado consistiu no *clicrbs.com.br*, que relacionado com o *estadao.com.br* representam o tipo de navegação de notícias. Em segundo lugar, encontrou-se o *google.com.br*, representando os mecanismos de busca.

Cabe ainda destacar o *facebook.com* como a rede social mais utilizada, *dropbox.com* para compartilhamento de arquivos, *msn.com* e *yahoo.com.br* para serviço de e-mail e o *ead06.proj.ufsm*

representando ambientes virtuais de ensino aprendizagem.

Com base nestes dados, pode-se perceber que os cinco sites mais acessados não pertencem ao domínio da universidade, o que pode caracterizar a má utilização da Internet e, consequentemente, possíveis perdas de produtividade. No entanto, a criação de uma regra taxativa bloqueando o acesso a esses sites pode prejudicar o desempenho de tarefas administrativas, de ensino ou pesquisa que dependam destes recursos, gerando novamente perdas de produtividade destes funcionários.

6.2.2 Planejar

Esta seção apresenta como realizou-se a etapa Planejar no Centro de Tecnologia da UFSM. A Seção 6.2.2.1 apresenta a atividade *Brainstorming*, onde extraiu-se as necessidades dos professores em relação ao gerenciamento. A Seção 6.2.2.2 o organograma criado a partir das necessidades do Centro de Tecnologia. A Seção 6.2.2.3, demostra o esquema de planejamento utilizado nos diagramas PERT e a Seção 6.2.2.4 apresenta-se o Plano de Ação 5W2H.

6.2.2.1 Brainstorming

Esta seção descreve a aplicação do *Brainstorming* Eletrônico. Realizou-se essa tarefa através de um questionário *online* semi estruturado que não exigia identificação, para evitar a inibição dos participantes. Planejou-se 14 questões com objetivo de acurar a relevância da implantação de um modelo de gestão de acessos à rede *Wireless* do Centro de Tecnologia, levantar diretrizes para elaboração da PUI e aspectos dinâmicos a serem utilizados como atributos contextuais nas PCAs. O questionário aplicado pode ser encontrado no anexo B.1.

Nesta etapa, obteve-se a participação de 13 professores dos cursos de graduação em Sistemas da Informação e Ciência da Computação. Na Figura 6.3 apresentam-se as perguntas e respostas referentes a questão 1 e 2.

Observa-se na Figura 6.3 que a maioria (84,61%) ministra duas ou três disciplinas. Apenas uma minoria (7,7%) ministra uma ou mais de três disciplinas. Percebe-se também que nas disciplinas ministradas pelos professores entrevistados, predomina a utilização de ambos os aspectos, teóricos e práticos (92,3% das disciplinas). Tal fato foi investigado com objetivo de verificar se as respostas dos professores se aplicariam apenas a aulas teóricas ou práticas.

A Figura 6.4 ilustra os resultados das questões 3 e 4. A questão 3 foi elaborada visando mensurar a importância da utilização da Internet através da perspectiva dos professores, enquanto que a questão 4 procurou verificar qual o tipo de aula mais se beneficiaria da utilização

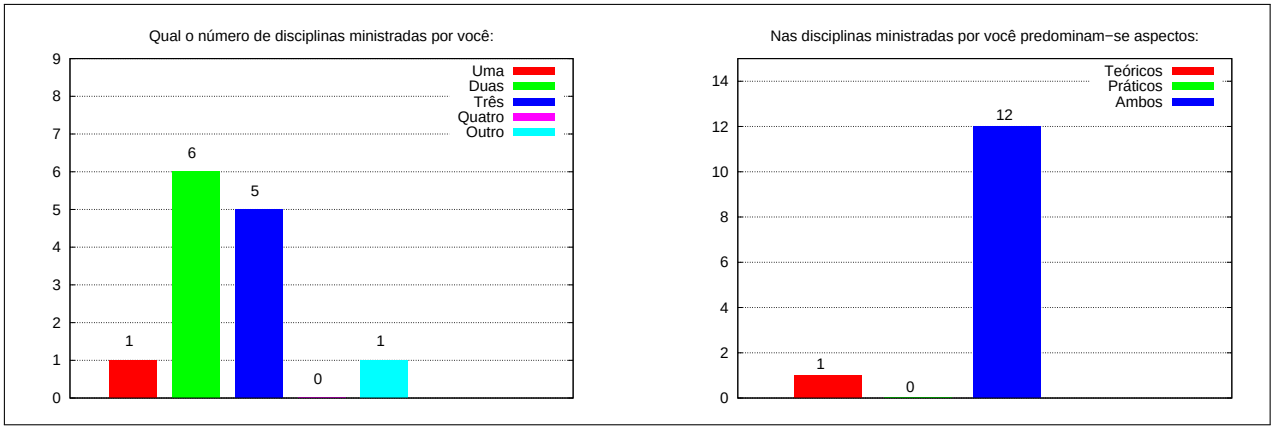


Figura 6.3: Questões para Averiguar o Número de Disciplinas e Aspectos Predominantes nas Disciplinas

da *Web*.

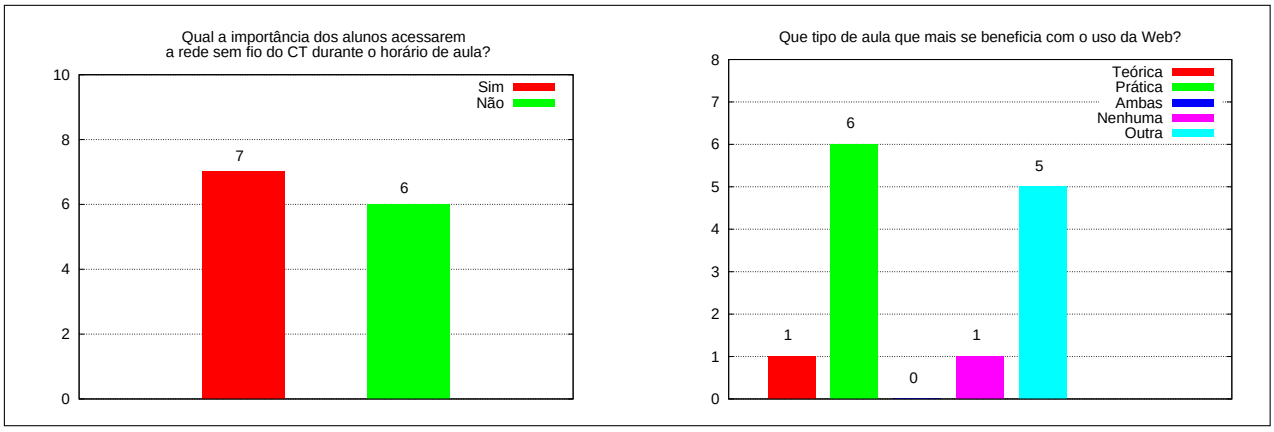


Figura 6.4: Questões Elaboradas para Acurar a Importância de um Modelo de Gestão de Acessos à Internet

O resultado da questão 3 indica um impate sobre a importância da utilização da Internet durante as aulas. Ao perguntar sobre os problemas desta implantação, os docentes manifestaram preocupação quanto a distração dos alunos, ou seja, a mesma preocupação encontrada nas empresas. No entanto, na questão 4, 92,30% dos participantes afirmaram que a utilização deste recurso pode beneficiar algum tipo de aula, o que justifica a utilização de um modelo de gestão de acessos à Internet no meio acadêmico.

A questão 5 (Figura 6.5) procurou verificar qual a relevância para os professores de haver PCAs adaptáveis às suas disciplinas. Na questão 6 buscou-se extrair a opinião dos professores quanto a relevância da utilização da Web para a potencialização do ensino dos alunos.

Percebe-se que dos entrevistados, 69,22% afirmaram que o uso da Internet é relevante ou muito relevante para a potencialização do aprendizado de sua disciplina. De maneira similar, 84,8% consideram importante ter PCAs adaptáveis as suas disciplinas, o que demonstra o inte-

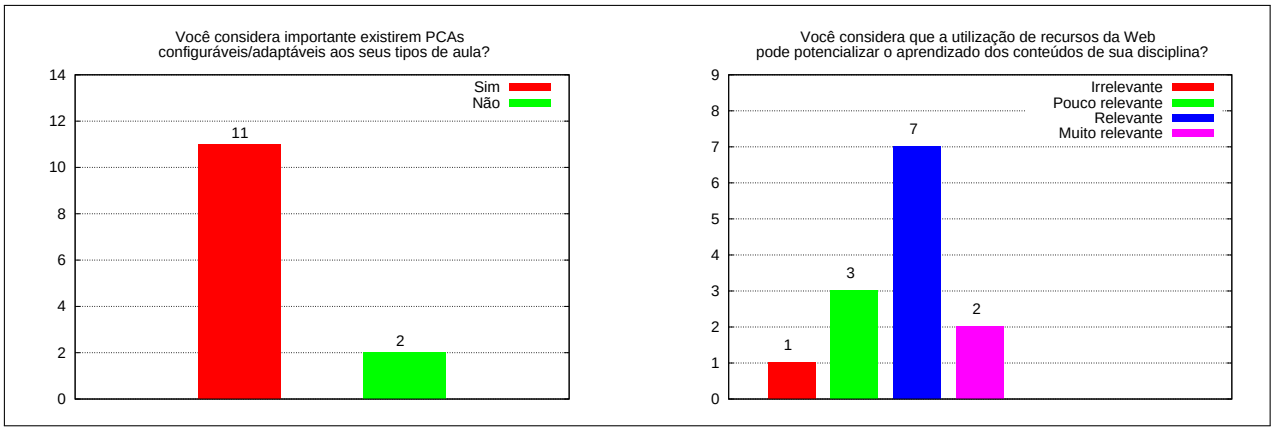


Figura 6.5: Questões para Mensurar a necessidade dos Professores Definirem PCAs configuráveis aos seus tipos de Aula e a Relevância deste Recurso na Potencialização da Aprendizagem dos Alunos

resse por permitir o acesso à Internet, porém sob controle do professor, que neste caso pode ser encarado como um empregador.

A questão 7 (Figura 6.6) analizou que tipos de navegação poderiam auxiliar nas atividades de ensino e aprendizagem. Classificou-se oito tipos de navegações e ainda disponibilizou-se as opções nenhuma e outro, possibilitando averiguar se os tipos de navegações previamente oferecidos atendiam as expectativas dos professores. A questão 8 procurou identificar a dinamicidade temporal envolvida nas disciplinas, dado que, conforme as normas da instituição de ensino um professor pode adotar dois tipos de intervalos, unindo os períodos e liberando mais cedo, ou realizando um intervalo a cada 50 minutos.

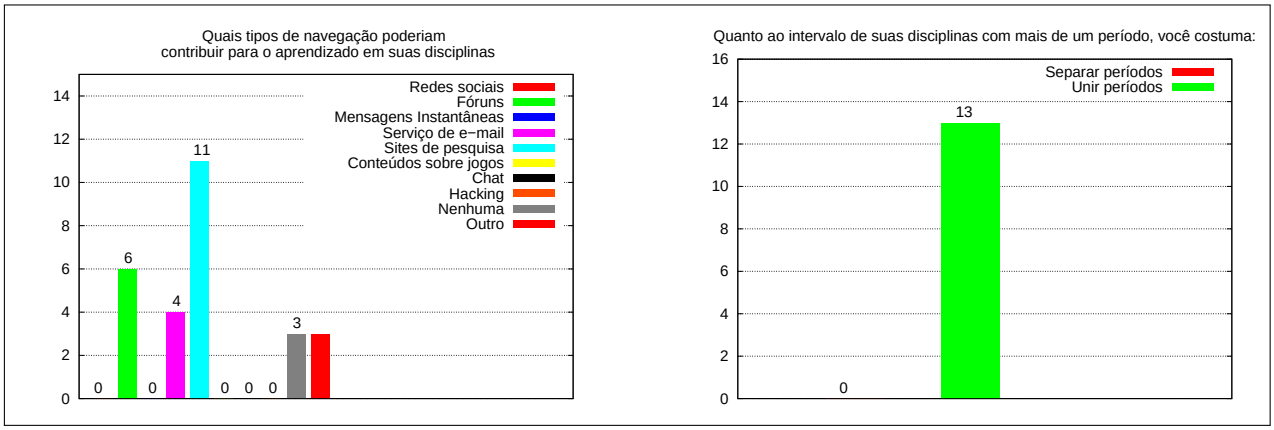


Figura 6.6: Questões para Auxiliar a Criação da PUI e PCA

O resultado da questão 7 indica que muitos participantes acreditam que a navegação em sites de pesquisa (84,6%), fóruns (46,15%) e serviço de e-mail (30,76%) poderiam contribuir para o aprendizado dos conteúdos de sua disciplinas. Já os 23,07% que citaram outra opção, sugeriram sites relacionados com sua disciplina e de ensino aprendizagem. Enquanto que na

questão 8, 100% dos professores afirmaram unir os períodos de aula para que os alunos tenham um intervalo maior.

Estes resultados justificam a inclusão da diretriz contida na PUI que permite o acesso a sites de pesquisa, fóruns e serviço de e-mail conforme a permissão do docente, enquanto que as sugestões de tipos de navegação servem como parâmetro para uma segunda iteração do modelo. Em relação aos aspectos dinâmicos das PCAs, o resultado da questão 8 determinou que horário em que a PCA vigoraria seria com a união dos períodos, ou seja, uma hora e quarenta minutos a partir do início da aula.

Para elaboração da questão 9 partiu-se da premissa que a utilização da *Web* é mais relevante conforme o tipo de aula ministrada. Dessa forma, pensou-se em justificar a criação de políticas diferenciadas conforme o tipo de aula ministrada, ou seja, que os alunos possuam acessos customizados para aulas teóricas e práticas. Já a questão 10 procurou verificar se o professor percebe a necessidade do aluno obter acesso diferenciado em cada tipo de aula. A Figura 6.7 apresenta o resultado desses questionamentos.

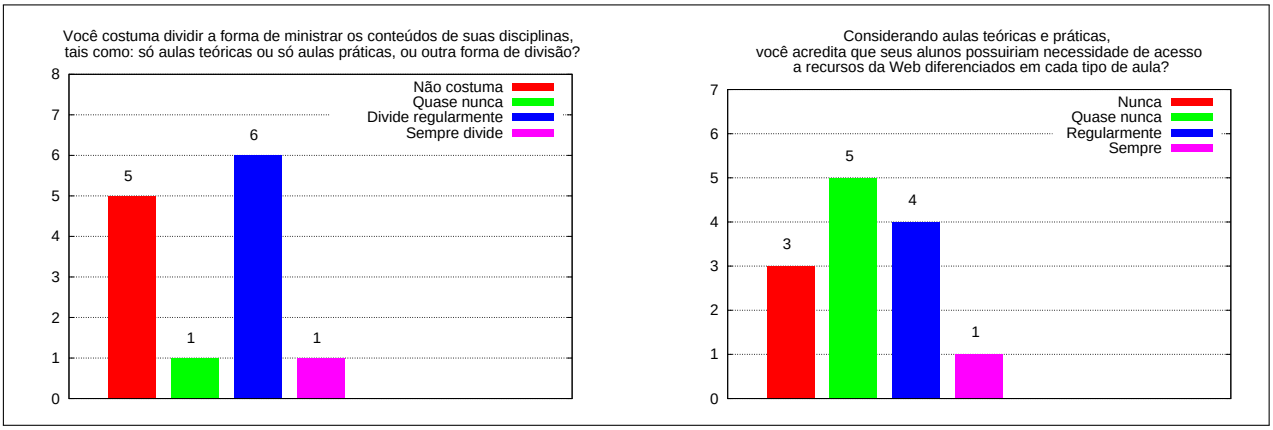


Figura 6.7: Questões Aplicadas para Justificar o Uso de PCAs Aplicáveis à Contextos Planejados pelos Docentes

Percebe-se que nas respostas da questão 9 que 69,23% dos professores possuem o hábito de em algum momento dividir a forma de ministrar os conteúdos de suas disciplinas, tais como aulas práticas ou teóricas. Aliando este fato com as respostas da questão 10, onde 76,92% dos docentes afirmaram que em algum momento desta divisão os alunos necessitam de acesso diferenciado à *Web*, pode-se perceber a necessidade de PCAs que se aplicam a contextos planejados pelos docentes.

Considerando a premissa citada, a questão 11 tentou mensurar a frequência com que os professores aplicavam atividades que poderiam ser melhor desempenhadas com o auxílio da

Internet. O objetivo deste questionamento consistiu em verificar a necessidade da utilização de PCAs sensíveis à atributos contextuais no ambiente de ensino. Complementarmente, a questão 12 buscou identificar a relevância de aplicar PCAs à rede *wireless*. A Figura 6.8 ilustra o resultado destes questionamentos.

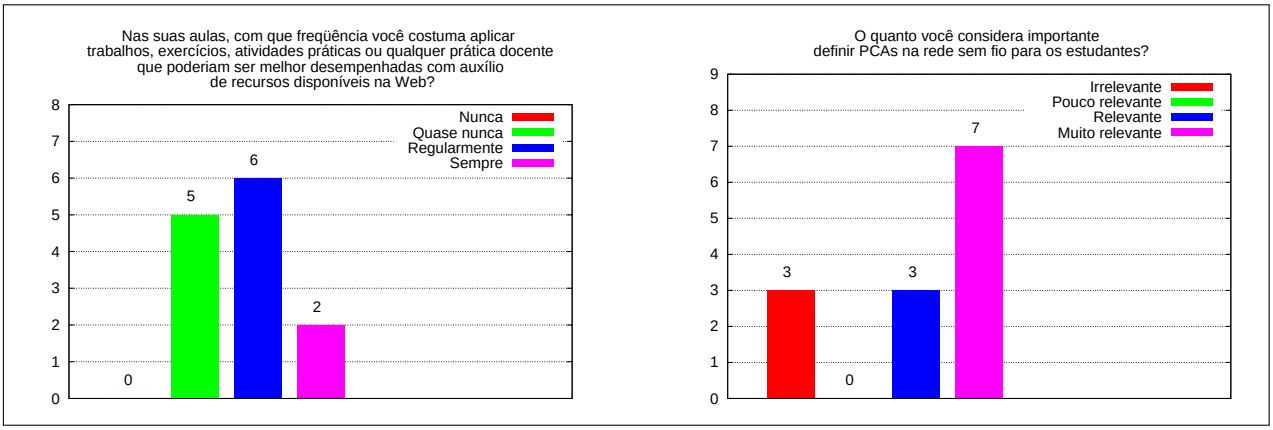


Figura 6.8: Questões para Acurar a Frequência que os Professores Aplicam Atividades que Podem ser Melhor Desempenhadas com auxílio da Web e a Relevância de Definir PCAs para Rede Sem Fio para os Estudantes

Observa-se na questão 11 que 100 % dos docentes afirmaram aplicar em algum momento práticas docentes que poderiam ser melhor desempenhadas com o auxílio da *Web*. Já o resultado da questão 12 mostra que 76,91% consideraram relevante ou muito relevante a utilização de PCAs no controle de acesso à rede sem fio, indicando que para um uso efetivo da *Web* em horário de aula os professores acreditam que PCAs são importantes.

A questão 13 buscou investigar a relevância de se ter PCAs customizadas às disciplinas dos professores do Centro de Tecnologia e a questão 14 buscou validar a importância da atualização das PCAs. A Figura 6.9 apresenta os resultados destes questionamentos.

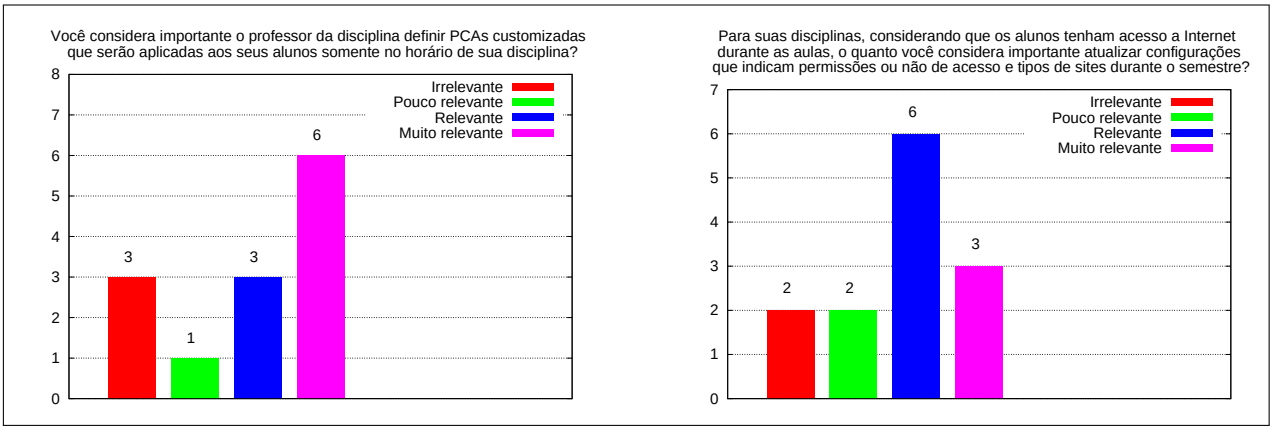


Figura 6.9: Questões que Justificam a Necessidade de Melhoramento Contínuo das PCAs Aplicáveis aos Horários das Disciplinas

Observa-se na questão 13 que 46% dos docentes afirmaram que a aplicação de PCAs customizadas às necessidades de suas disciplinas é muito relevante, o que justifica a elaboração e gerenciamento de políticas para cada disciplina, ao invés de uma PCA tradicional. Na questão 14 da mesma figura, observa-se que 69,23% afirmaram que esta medida é relevante ou muito relevante, enquanto 38,46% consideram irrelevante ou pouco relevante. Com esta informação, pode-se notar que os docentes entrevistados visualizam a necessidade da melhoramento contínuo de políticas que objetivam gerir a má utilização da *Web* no ambiente acadêmico.

Com a aplicação deste questionário, pode-se concluir que existe a necessidade de gerir os acessos à rede *Wireless* do Centro de Tecnologia. Conseguiu-se extrair como diretriz de planejamento da PUI que o acesso à sites de pesquisa, fóruns e serviços de e-mail pode ser liberado durante as aulas, ou seja, que estas opções estejam disponíveis no SGPCA. E ainda determinar que os aspectos temporais referente o intervalo dos alunos, deve unir os períodos e gerar apenas um intervalo de vinte minutos, de forma que a PCA gerada pelo SGPCA seja aplicada por uma hora e quarenta minutos a partir do início da aula.

6.2.2.2 Organogramas

Esta seção apresenta o organograma construído para realização do gerenciamento das PCAs. Conforme COPLAD/PROPLAN/UFSM (2009), o organograma da Universidade possui a estrutura da Figura E.1 do anexo E. No entanto, como em tal atividade procurou-se abranger exclusivamente as necessidades do cenário escolhido, considerou-se como perfis principais os Alunos, Professores e Técnicos administrativos, como ilustra a Figura 6.10.

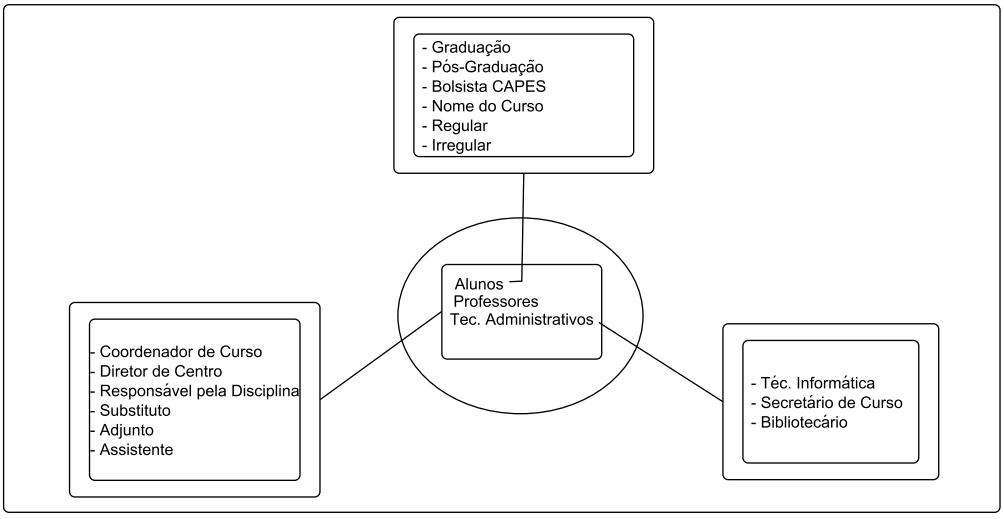


Figura 6.10: Organograma Elaborado para o Ambiente de Testes

O perfil "Alunos"possui uma associação com outras especificidades de alunos, como de Graduação, Pós-graduação, Bolsista CAPES, Regular, Irregular e Nome do Curso em que o mesmo se encontra matriculado. Da mesma forma nota-se a associação de professores com Coordenador de Curso, Diretor de Centro, Assistente, Adjunto, Substituto e Responsável pela Disciplina. A definição destes perfis foi expandida com base nos sujeitos presentes nos questionários aplicados, sendo eles servidores e alunos. Estes perfis em conjunto com as informações obtidas na fase *Brainstorming*, passou-se a fase de diagramas PERT.

6.2.2.3 Diagramas PERT

Esta seção apresenta como um professor pode utilizar diagramas PERT na etapa de planejamento do modelo para auxiliá-lo na gestão da má utilização da Internet. Como o período de validação consistiu no final do semestre, onde os professores ficam muito sobrecarregados com as avaliações do semestre, essa etapa não foi implantada no ambiente real, todavia pretende-se implantá-lo no primeiro semestre de 2012. Para explicar como essa tarefa pode ser realizada, utilizou-se um plano de ensino aplicado na disciplina de Banco de Dados 2 no segundo semestre de 2011 na Universidade de Cruz Alta para demonstrar como essa etapa pode ser realizada. O plano de ensino pode ser encontrado no anexo D.

Para criação de um diagrama PERT primeiramente torna-se necessário identificar as principais fases de um projeto. Com objetivo de extrair essas informações do plano de ensino, observa-se no tópico *Metodologia e suas estratégias* que a disciplina foi ministrada tendo como estratégias os instrumentos de explanação oral do conteúdo teórico, exercícios envolvendo os conteúdos da aula, debate sobre as soluções dos exercícios da aula, provas teóricas descritivas, atividades práticas em laboratório e projeto e desenvolvimento prático de uma base de dados distribuída.

Com base nessas estratégias, pode-se notar que ambos os Bimestres estão organizados com base em três fases: Teórica, Prática e Avaliativa. Pode-se organizar essas estratégias como atividades do diagrama PERT, de modo que na fase Teórica contenha as atividades: Aula Expositiva, Exercícios Teóricos e Debate sobre Resolução dos Exercícios. Na fase Prática: Aula Expositiva, Aulas Práticas em Laboratório, Trabalho Prático e Debate sobre Resolução dos Exercícios. Enquanto que na fase Avaliativa: Avaliação Prática e Avaliação Teórica.

Para determinar as tarefas para cada atividade, considere o *Conteúdo programático* do plano de ensino em anexo. Considerando os ítem do conteúdo como uma tarefa das atividades Exer-

cícios Teóricos, Atividade Prática em Laboratório e Trabalho Prático, a Figura 6.11 ilustra a associação entre fases, atividades e tarefas.

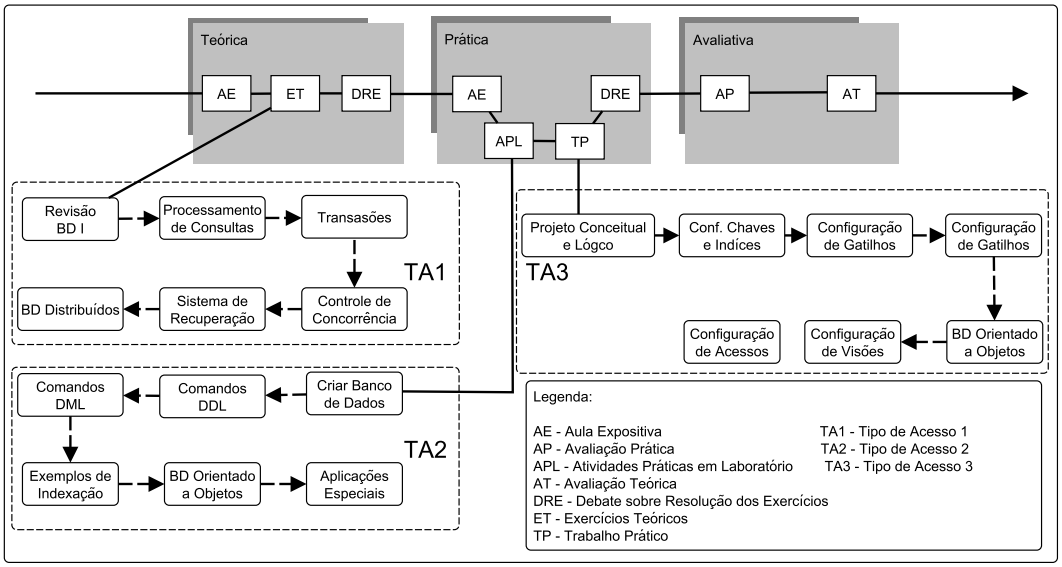


Figura 6.11: Diagrama PERT para Disciplina de Banco de Dados

Pode observar na Figura 6.11 que para cada atividade apresentada, associou-se um tipo de acesso. Neste caso, para o Tipo de Acesso 1 e 2 poderia ser disponibilizado o acesso ao material on-line disponibilizado na disciplina de Banco de Dados 1 e a livros disponibilizados e comercializados na *Web*. No Tipo de Acesso 3, poderia ser disponibilizado acesso a documentação digital do Postgresql e fóruns sobre esse SGBD.

Com a criação de um diagrama PERT a partir do um plano de ensino de Banco de Dados 2, pode-se notar como se extrai fases, atividades e tarefas de um plano de ensino para realizar o planejamento das atividades que serão ministradas em uma disciplina. Com essa etapa de planejamento torna-se mais fácil associar tipos de navegação necessários para a realização das tarefas planejadas com objetivo de inibir a má utilização da Internet.

6.2.2.4 Plano de Ação 5W2H

Esta seção apresenta o plano de ação desenvolvido para o primeiro semestre da disciplina de Banco de Dados 2, conforme o plano de ensino apresentado no anexo D. Dessa forma, o plano de ação apresentado na Tabela 6.1 foi elaborado considerando as atividades Exercícios Teóricos, Aulas Práticas em Laboratório e Trabalho Prático do Diagrama PERT, apresentado na seção anterior.

Na Tabela 6.1, percebe-se que extraiu-se da fase Teórica a tarefa Exercícios Teóricos e da

Tabela 6.1: Plano de Ação 5W2H para a Disciplina de Banco de Dados 2

Projeto: Disciplina de Banco de Dados							
O QUÊ		POR QUÊ	COMO				
item			item	Quem	Necessidade de Acesso	Data Inicial	Data Final
1	Responder Exercícios Teóricos	Para debater sobre as soluções dos exercícios	1.1	Alunos	1.1, 1.2 e 1.3		
1.1	Acessar Conteúdo Disponibilizado	1	1.1.1		http://www.ctec.unicruz.edu.br/	25/8/2011	6/10/2011
1.2	Acessar Livros On-line	1	1.2.1		http://books.google.com.br		
1.3	Acessar Sites de Pesquisa	1	1.3.1		http://www.google.com.br		
1.4	Acessar Lojas On-line de Livros	Caso o aluno queira adquir um exemplar	1.41		http://www.amazon.com/Computers-Internet-Books/		
2	Estudo de caso Firebird	Exercícios de fixação	2.1		2.1 e 2.2		
2.1	Acessar Documentação	2	2.1.1		http://www.firebirdsql.org/	1/9/2011	1/9/2011
2.2	Acessar Fóruns de Pesquisa	2	2.2.1		http://scriptbrasil.com.br/forum/		
3	Estudo de caso PostgreSQL	Fixar conteúdos sobre Indexação e hashing, índices ordenados, arquivos de índice Árvore-B, Hashing Estático e Dinâmico e índice em SQL	3.		3.1 e 3.2	15/9/2011	15/9/2011
3.1	Acessar Documentação	3	3.1.1		http://www.postgresql.org/		
3.2	Acessar Fóruns de Pesquisa	3	3.2.1		http://scriptbrasil.com.br/forum/		
4	Pesquisar sobre Trabalho Prático	Possibilitar Pesquisas Finais sobre o Trabalho	4.1		4.1, 4.2 e 4.3		
4.1	Acessar Fóruns de Pesquisa	4	4.1.1		http://scriptbrasil.com.br/forum/	6/10/2011	12/10/11
4.2	Acessar Documentação do Postgresql	4	4.2.1		http://www.postgresql.org/		
4.3	Acessar Exemplos de Código	4	4.3.1		http://www.vivaolinux.com.br/		
4.4	Acessar Sites de Pesquisa	4	4.4.1		http://www.google.com.br		

Prática as tarefas Atividades Práticas em Laboratório e Trabalho Prático, no plano de ação essas informações aparecem como itens 1, 2, 3 e 4. Percebe-se que, em contraste com os Diagramas PERT, o plano de ação apresenta quais sites devem ser utilizados em cada tarefa e ainda permite definir datas em que cada recurso estará disponível. Esta associação de recursos, datas e horários representa a extração de atributos dinâmicos que estarão contidos na PCAs de sua aula e agrega fina granularidade ao gerenciamento.

Um exemplo disto são os ítens 2 e 3, onde se define o acesso ao domínio *ScriptBrasil, Firebird e PostgreSql* somente durante o dia que a aula será realizada. Já no item 4, apesar de não descrito expressamente no plano de ensino, liberou-se acesso aos sites que auxiliam na elaboração do trabalho prático durante as aulas para que os alunos possam finalizar as atividades em sala de aula.

6.2.3 Executar

Esta seção apresenta como empregaram-se as diretrizes das PUIs e PCAs sensíveis à atributos contextuais no filtro de acesso à Internet. Desse modo, com base na etapa de planejamento apresentada na seção anterior elaborou-se o modelo de PCA apresentado no anexo A, sendo que para gerar as PCAs os docentes utilizaram o *software* de gestão SGPCA.

Como os docentes afirmaram que costumavam unir períodos de aula adjacentes, permitindo aos alunos um intervalo mais longo, o modelo de PCA aplica as regras definidas pelos docentes em um único intervalo, quando houver mais de um período em sequência da mesma disciplina.

Quando não existirem mais de um período em sequência, a PCA entra em vigor por quarenta minutos, liberando os alunos por 10 minutos, dado o tamanho do período de 50 minutos na UFSM. Mas períodos em que os alunos não estão em aula, vigora a PCA definida pela direção do Centro de Tecnologia. Em tal PCA determinou-se aos alunos a impossibilidade de acesso a sites de pornografia e compartilhamento de arquivos. A direção do centro definiu que o controle de acesso através de PCAs seria aplicado apenas aos alunos da instituição.

Na fase Executar também foi elaborada, com base no organograma apresentado na seção 6.2.2.2, a PUI apresentada no anexo C, onde, visando empregar os critérios eficazes desta abordagem, criou-se um documento consientizando os usuários de seus deveres e direitos do Centro de Tecnologia em aplicar medidas disciplinares. Mais precisamente, esclarecendo que todos os usuários do sistema, alunos e servidores, terão seus acessos à Internet monitorados e em caso de infrações o sigilo desta navegação poderia ser quebrado. Além disso, tal documento deixa

claro que a utilização da Internet deve ser realizada segundo os propósitos acadêmicos.

Para oficializar a concordância dos usuários quanto as diretrizes estabelecidas na PUI, foi inserido uma mensagem na página de autenticação do portal de acessos sobre os termos de utilização e um *link* para o documento. Mais detalhes sobre a PUI podem ser encontrados no anexo C, enquanto que o modelo de PCA utilizado pode ser encontrado em sua totalidade no anexo A.

6.2.4 Verificar

Esta seção apresenta como foi mensurada a eficácia das medidas de segurança adotadas. Tanto a PUI, quanto a PCA apresentadas na seção anterior vigoraram por duas semanas. Para mensurar tal eficácia, gerou-se relatórios dos acessos à Internet e aplicou-se um questionário, cujo objetivo consistiu em verificar se após a implantação do modelo mudou a relevância dos alunos utilizarem a Internet durante as aulas e extrair sugestões para aprimorar o gerenciamento. Para que se pudesse comparar com a etapa Planejar, utilizou-se a coleta dos mesmos dados referente as duas semanas de implantação, sendo que esta realizou-se no período de 28 de Novembro à 11 de Dezembro de 2011.

Através da ferramenta *ntop*, realizou-se um acompanhamento dos tipos de navegação mais utilizados durante o período de aplicação do modelo. O referido monitoramento é ilustrado na Figura 6.12. Também utilizou-se uma ferramenta do grupo de pesquisa que permite a geração de relatórios por usuários para que se pudesse detectar a má utilização da *Web*.

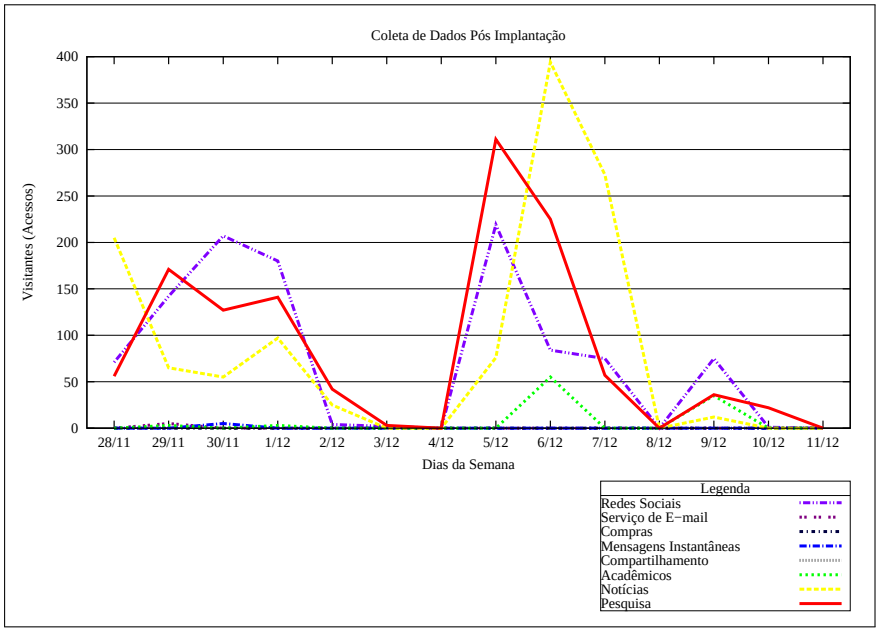


Figura 6.12: Sites Mais Acessados a Partir da Aplicação do Modelo

Na Figura 6.12 pode se observar que os três tipos de navegação que mais se destacaram consistiram em sites de notícias, pesquisa e redes sociais. Dentre os sites destes tipos de navegação, cabe salientar o *Facebook.com* e *Orkut.com.br* como redes sociais, *Gmail.com* e *Yahoo.com.br* como serviço de e-mail e o ambiente de ensino/aprendizagem e o site da universidade como sites acadêmicos. Verificou-se no diretório de políticas geradas pelo SGPCA que alguns professores não liberaram o acesso a todos os tipos de navegação, os mais liberados foram serviços de e-mail, sites de pesquisa e fóruns. Como o tipo de navegação mais acessada foram as redes sociais, pode-se observar que conseguiu-se obter um acesso diferenciado a rede sem fio, ou seja, apesar de nenhum professor permitir o acesso à redes sociais às suas aulas, fora delas os alunos tinham acesso a esse tipo de navegação. Portanto pode-se afirmar que se obteve uma granularidade fina no controle de acesso.

Como mencionado anteriormente, outro indicador utilizado na etapa verificar consistiu na aplicação de questionários. A elaboração destas questões objetivaram verificar se ocorreram mudanças na perspectiva dos professores quanto a utilização de PCAs no controle de acesso à rede sem fio. Como também, receber *feedback* para aprimoramentos no sistema. O questionário completo pode ser encontrado no anexo B.2.

O questionário foi aplicado ao mesmo grupo de 33 docentes da etapa Planejar, onde obteve-se a participação de 12 professores, todavia como o questionário não exigia identificação não se sabe se foram os mesmos que participaram da primeira coleta. Dessa forma, na questão 1 da Figura 6.13 pode-se observar que 83,4% afirmaram ser importante que os alunos tenham acesso a rede sem fio durante o horário de aula.

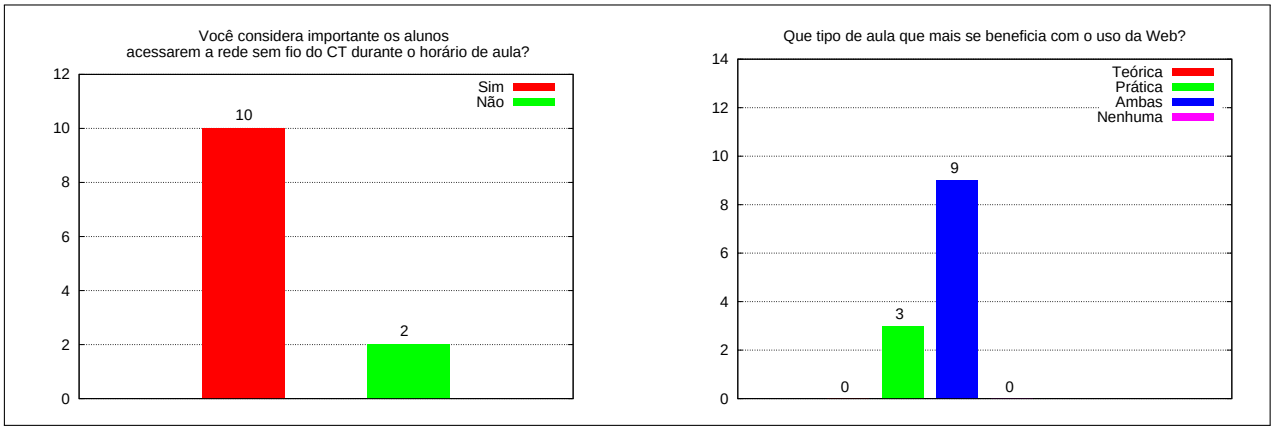


Figura 6.13: Questões para Verificar se Ocorream Mudanças Quanto a Importância dos Alunos acessarem a Rede Sem Fio e do Tipo de Aula que Mais se Beneficia com a Utilização da Web

Comparando esse resultado com o impate obtido na questão 3 durante o *Brainstorming*,

percebe-se que após a implantação do modelo ocorreu uma mudança significativa na opinião dos professores, o que indica uma melhoria na cultura da segurança da informação na instituição. Na questão 2, comparando com a questão 4 da etapa Planejar, pode-se dizer que não ocorram mudanças. Pois a maioria continuou acreditando que o uso da Internet pode beneficiar algum tipo de aula.

As questões 3 e 4 (Figura 6.14) são as mesmas perguntas 5 e 6 aplicadas na etapa Planejar. Considerando os resultados da questão 3, percebe-se que não ocorreram mudanças de opinião. Pois nas duas etapas a maioria (84,8% e 91,66%) considerou ser importante ter PCAs configuráveis aos seus tipos de aula, o que confirma a necessidade da implantação do modelo.

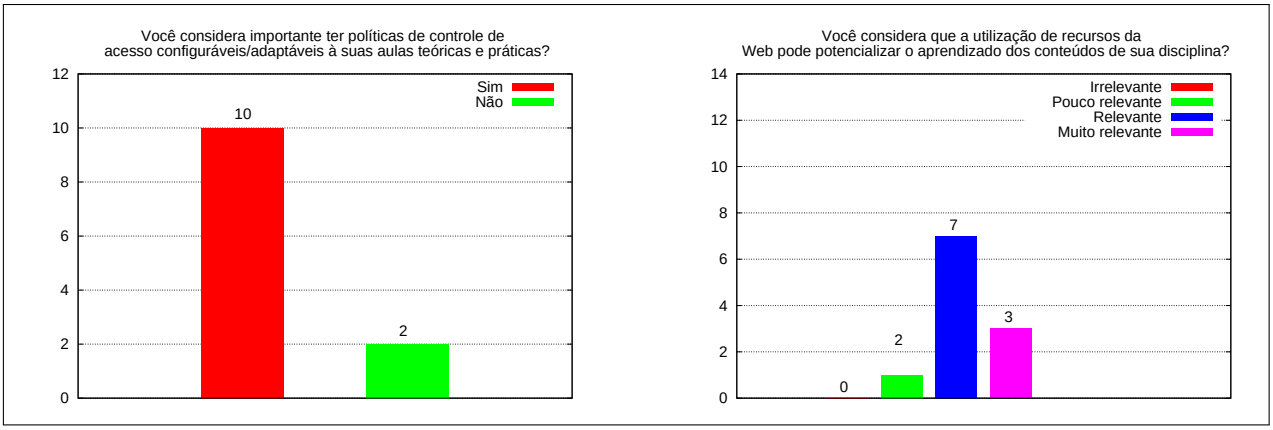


Figura 6.14: Questões para Investigar se Ocorream Mudanças Quanto a Relevância de se Ter PCAs Adaptáveis aos Tipos de Aula e da Potencialização da Aprendizagem dos Alunos com Utilização deste Recurso

Em relação a questão 4, notam-se mudanças pois na etapa Planejar 69,22% dos entrevistados afirmaram ser relevante ou muito relevante para potencialização do aprendizado dos conteúdos das disciplinas, na segunda aplicação este número cresceu para 100% dos participantes, o que também indica uma melhoria na cultura da segurança da informação na instituição.

Na questão 5 (Figura 6.15) procurou-se reformular a questão 7 do questionário aplicado durante a etapa Planejar, acrescentando às opções de tipos de navegação ambientes virtuais de aprendizagem e sites relacionados com a disciplina que foram sugeridas. Na questão 6 procurou-se mensurar a necessidade de atualização de PCAs após a aplicação das PCAs, justificando a necessidade de aprimoramento contínuo destas políticas.

Comparando os resultados da questão 5 com sua similar aplicada na etapa Planejar, percebe-se que os mesmos tipos de navegação foram votados. No entanto, quanto aos sites relacionados com a disciplina, exige uma atualização no SGPCA para que cada docente insira os sites que considere importante. Já na questão 6, pode-se observar que 75% dos participantes manifesta-

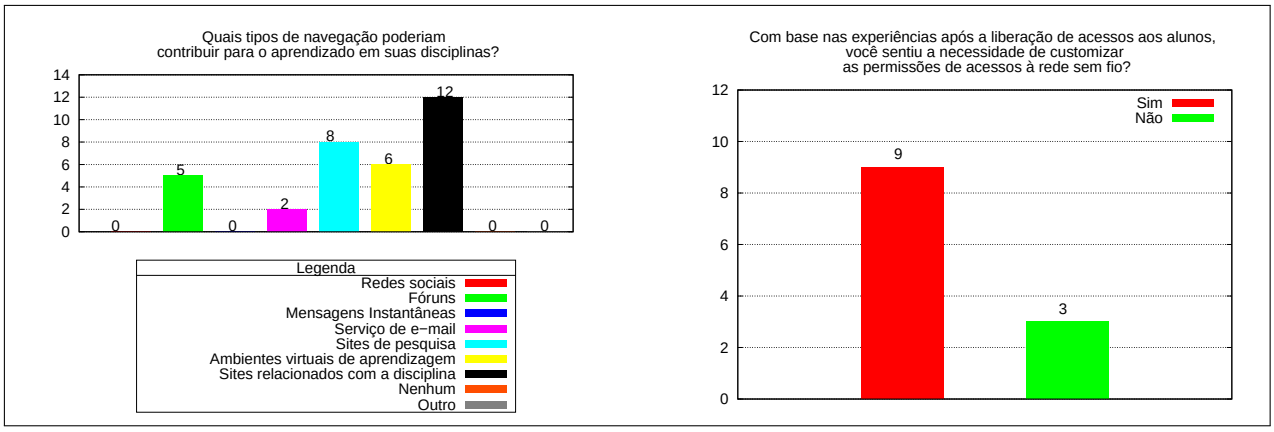


Figura 6.15: Questões para Acurar se Ocorream Mudanças quanto aos Tipos de Navegação que Podem Contribuir para o Aprendizado dos Conteúdos e a Necessidade de Customizar a PCA Após a Implantação do Modelo

ram a necessidade de atualização de PCAs, o que justifica o gerenciamento contínuo de PCAs.

A questão 7 foi elaborada de forma dissertativa, para que o docente pudesse expressar possíveis carências na utilização do *software* de geração de PCAs. Dentre as respostas dos professores obteve-se: a possibilidade de delegação de tarefas, o controle individual de alunos e a possibilidade de habilitar e desabilitar o acesso dos alunos caso estejam utilizando a rede para outros fins que não os da aula. Ainda com o objetivo de verificar se ocorreram mudanças na opinião dos professores quanto a utilização de PCAs, as questões 12 e 13 da etapa foram reaplicadas, tendo agora a numeração 8 e 9 (Figura 6.16).

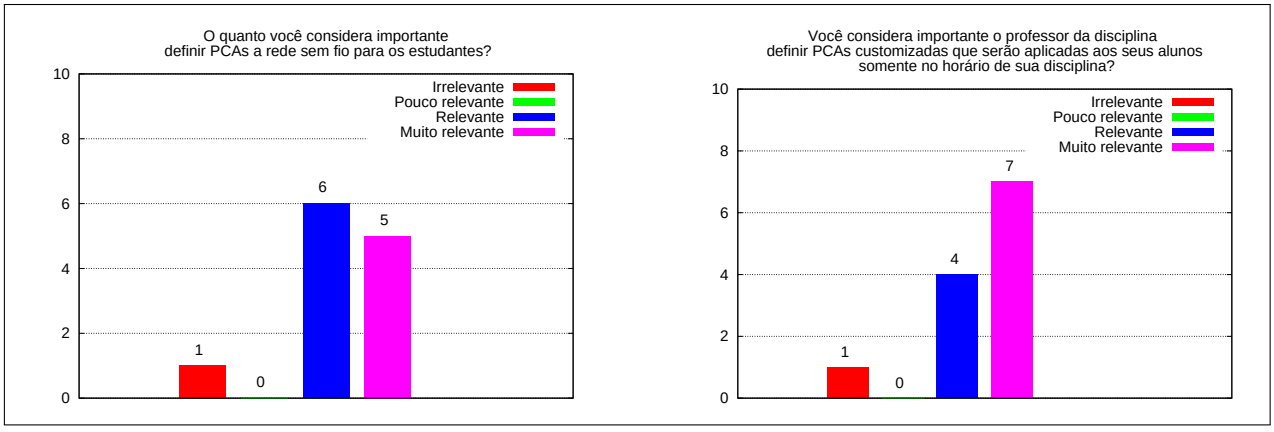


Figura 6.16: Questões para Verificar se Ocorream Mudanças Quanto a Importância de Definir PCAs Considerando a Utilização do Protótipo e do Professor da Disciplina Definir PCAs Aplicáveis aos Seus Alunos

Comparando os resultados dessas questões com suas similiares da primeira etapa, percebe-se uma melhora significativa. Pois no resultado da questão 8, 91,66% dos participantes afirmaram ser relevante ou muito relevante definir PCAs para rede sem fio dos estudantes, con-

tra 76,91% da etapa anterior. Na questão 9, obteve-se o mesmo percentual de participantes (91,66%) manifestando ser relevante ou muito relevante ter PCAs customizadas, aplicáveis somente a sua disciplina. O resultado dessas duas questões demonstra que o envolvimento dos professores incrementou a importância da gestão dos acessos à Internet.

Ao reutilizar perguntas empregadas na etapa Planejar pode-se observar no resultado das questões 1, 4, 8 e 9 que ocorreram mudanças de opiniões positivas, ou seja, ocorreu uma valorização da gestão de acessos à rede sem fio. Em relação as melhorias para o próximo ciclo do modelo, extraiu-se as seguintes sugestões de aprimoramento do SGPCA: possibilidade de delegação de tarefas, controle individual de alunos e a possibilidade de habilitar e desabilitar o acesso dos alunos caso estejam utilizando a rede para outros fins que não os da aula. Esses resultados demonstram a eficiência do modelo em prover um ciclo de melhoria contínua.

6.2.5 Agir

Esta seção apresenta possíveis medidas disciplinares ou de incentivo que poderiam ser empregadas visando estimular os estudantes a utilizarem a Internet de forma direcionada aos propósitos das disciplinas. Pensou-se em sugerir aos docentes a associar ao processo de avaliação de suas disciplinas uma pontuação, mesmo que simbólica, pela boa utilização da Internet em sala de aula.

Aplicando esta sugestão os alunos que não utilizaram de forma coerente este recurso não ganhariam esta pontuação, o que representa a medida disciplinar. Enquanto que os alunos que usaram esta tecnologia conforme os propósitos definidos pelos docentes receberiam estes pontos, caracterizando a medida de incentivo. Desta forma, aplicando estes tipos de medidas, se incrementaria a cultura da utilização da *Web* com os fins da instituição, neste caso o ensino.

Entretanto, como o período de aplicação da proposta consistiu nas duas últimas semanas de aula, não obteve-se a oportunidade de avaliar estes dados em tempo hábil para que as informações de acessos fossem entregue aos docentes e estes pudessem adotar estas medidas.

6.3 Considerações Finais

Este capítulo apresentou um estudo de caso demonstrando a aplicação de um ciclo do modelo proposto para gestão da má utilização da Internet. Sendo que neste utilizou-se a rede sem fio do Centro de Tecnologia da Universidade Federal de Santa Maria como objeto de investigação. Mostrou-se que para tornar possível tal gestão, elaborou-se um protótipo de *software*

apartir da alteração do código fonte do servidor *Proxy Squid*. Com esta alteração, tornou-se possível técnicamente aplicar PCAs sensíveis à atributos contextuais, capazes de representar as necessidades do ambiente acadêmico.

Para que servisse de parâmetro à etapa Planejar, realizou-se uma coleta de acessos *Web* antes da implantação da gestão, onde constatou-se que alguns tipos de navegação consideradas como indevidas estavam sendo acessados, entre elas redes sociais e lojas virtuais. Após o emprego do modelo, aplicou-se outra coleta onde pode-se perceber que alguns acessos considerados indesejáveis continuaram ocorrendo, mas durante os intervalos de aula. Isto demonstra que adquiriu-se a granularidade discutida por Wilson (2009), onde discute-se que dependendo da situação, um acesso considerado pela maioria como indesejado em determinado momento pode potencializar a produtividade dos trabalhadores.

O resultado dos questionários aplicados no *Brainstorming* Eletrônico da etapa Planejar e na etapa Verificar indicam que, ao contrário do que se pensava, tanto aulas teóricas quanto práticas podem ser potencializadas com a utilização da Internet. Com estes conseguiu-se coletar informações para aprimoramentos do SGPCA tais como: inserir o tipo de navegação à ambientes de ensino e aprendizagem e sites relacionados com a disciplina; possibilidade de delegação de tarefas; controle individual de alunos e a possibilidade de habilitar; e desabilitar o acesso dos alunos caso estejam utilizando a rede para outros fins que não os da aula.

Percebeu-se uma mudança de opnião dos docentes referente a importância de se empregar PCAs à rede *Wireless* do CT, o que indica que a utilização do modelo proporciona um incremento na cultura da gestão da segurança da informação na instituição. Definiu-se aspectos dinâmicos para as PCAs, referente ao intervalo das disciplinas, tal decisão interfiriu no projeto do modelo de PCA utilizada pelo SGPCA.

Criou-se um organograma específico para o ambiente do estudo de caso, contendo perfis de professores, alunos, técnicos administrativos e alunos, entre outros. Para a criação dos Diagramas PERT utilizou-se somente os perfis aluno e professor para demonstrar como um docente pode planejar suas aulas tendo como base um plano de ensino, onde percebeu-se que esta estratégia trata-se de uma forma rápida e fácil de planejar quais recursos devem ser associados as tarefas planejadas para que uma atividade seja realizada.

Utilizando as fases, atividades e tarefas do Diagrama PERT projetou-se um plano de ação 5W2H que apresentou como este provê facilidades quanto a especificação direta de recursos da Internet serão permitidos em determinada data ou horário.

Quanto a fase Executar, utilizou-se o SGPCA para minimizar o custo da elaboração e manutenção das PCAs e aplicou-se a PUI elaborada na etapa Planejar. Enquanto que na fase Agir apresentou-se possíveis medidas disciplinares e de incentivo para o ambiente acadêmico.

7 CONCLUSÕES

Nesta dissertação abordou-se o problema da má utilização da Internet, que consiste em uma ameaça à produtividade nas empresas. Apresentou-se que dentre as estratégias utilizadas para tratar essa ameaça, o emprego de PUI tornou-se a mais utilizada. No entanto, o emprego de PUI apresenta dificuldades quanto ao cumprimento das diretrizes, o que levou a alguns autores empregar PCAs para contornar essa carência.

Mostrou-se que PCAs sensíveis a atributos contextuais podem possuir granularidade fina suficiente para empregá-las no gerenciamento da má utilização da Internet, apesar de serem mais complexas para elaboração e oferecerem risco de tornar-se obsoletas com o passar do tempo.

Este trabalho propôs um Modelo de Gestão para Prevenção da Má Utilização da Web que provê um processo de gestão constituído por um ciclo de melhoria contínua aplicável à manutenção de PCAs com granularidade fina, bem como propôs também o software SGPCA que auxilia na aplicação do modelo, o qual minimiza o custo do processo de elaboração e manutenção das PCAs. Em relação a este *software* apresentou-se um estudo comparativo do SGPCA com os *softwares MyHotSpot*, *Mikrotik* e *Squid*, onde demonstrou-se que o *software* proposto emprega PCAs com granularidade mais fina que os demais, possui um método de autenticação integrável com outros possíveis sistemas das instituições, não exigindo conhecimento de gerência de rede para criação das PCAs e ainda tendo a vantagem de ser uma solução livre.

Ambas as propostas foram validadas através de um estudo de caso realizado na rede sem fio do Centro de Tecnologia da Universidade Federal de Santa Maria. Através da aplicação de *Brainstorming* Eletrônico, com a participação de 13 docentes na Etapa Planejar e 12 na Etapa Verificar, o estudo apresentou que tanto aulas teóricas quanto práticas podem ser potencializadas com a utilização da Internet. Com esta ferramenta também coletou-se *feedbacks* quanto ao aprimoramento do SPGCA, promovendo a iteração do modelo.

Também se identificou uma mudança significativa sobre a opnião dos docentes quanto a importância de se empregar PCAs à rede *Wireless* do CT, o que indica que a utilização do modelo proporciona um incremento na cultura da gestão da segurança da informação na instituição. Não investigou-se o impacto da aplicação da proposta em relação a da perspectiva dos alunos, devido a limitação do trabalho. Acurou-se também, que tanto aulas teóricas quanto práticas podem ser potencializadas com a utilização da Internet.

Observou-se que a técnica de *Brainstorming* possui maior empregabilidade no levantamento de diretrizes para compor a PUI e na coleta de informações para aprimorar o gerenciamento. Já a utilização de Organogramas, Diagramas PERT e Plano de Ação 5W2H apresentam uma forma ágil e fácil para realizar o planejamento da associação dos perfis, recursos, tarefas e atributos dinâmicos que irão compor a PCA.

As coletas de tráfego empregadas antes da implantação do modelo e na Etapa Planejar, indicam que o estudo conseguiu obter como resultado a granularidade no acesso à Internet discutida por Wilson (2009). Visto que, mesmo após o emprego das PCAs no filtro de acesso, em momentos não especificados nas PCAs, ocorreram acessos que podem ser considerados inapropriados.

Considerando as propostas tradicionais empregadas pelas empresas, onde libera ou se nega o acesso à tipos de navegação. O emprego do modelo proposto serve como uma alternativa moderadora, permitindo espeficiar PCAs flexíveis e customizadas conforme as necessidades da empresa, reduzindo as perdas de produtividades associadas à má utilização da *Web*. Este fato aponta que em uma empresa onde existem funcionários que praticam atividades inapropriadas na *Web* e necessita que alguns profissionais tenham acessos diferenciados para potencializar o desempenho de suas tarefas no ambiente de trabalho.

Em trabalhos futuros se buscará empregar técnicas de gerência de redes para analizar se a gestão empregada afeta o desempenho da rede, procurar mensurar o impacto que a gestão de acessos à rede causa nos usuários do modelo, comparar a solução empregada neste trabalho com *softwares* comerciais e ainda empregar a gestão no início do semestre.

REFERÊNCIAS

AJZEN, I. The theory of planned behavior. **Organizational Behavior and Human Decision Processes**, [S.l.], v.50, n.2, p.179 – 211, 1991. Theories of Cognitive Self-Regulation.

ALAMPAY, E. A.; HECHANOVA, M. R. M. Monitoring Employee Use of the Internet in Philippine Organizations. **The Electronic Journal on Information Systems in Developing Countries**, [S.l.], v.5, p.1–20, 2010.

ANANDARAJAN, M. Profiling Web Usage in the Workplace: a behavior-based artificial intelligence approach. **J. Manage. Inf. Syst.**, Armonk, NY, USA, v.19, p.243–266, July 2002.

ARNESEN, D.; WEIS, W. Developing an effective company policy for employee Internet and email use. **Journal of Organizational Culture Communications and Conflict**, [S.l.], p.53–65, 2007.

BARRERA, D.; KAYACIK, H. G.; OORSCHOT, P. C. van; SOMAYAJI, A. A methodology for empirical analysis of permission-based security models and its application to android. In: ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, 17., 2010, New York, NY, USA. **Proceedings...** ACM, 2010. p.73–84. (CCS '10).

BOCK, G.-W.; HO, S. L. Non-work related computing (NWRC). **Commun. ACM**, New York, NY, USA, v.52, p.124–128, April 2009.

CASE, C. J.; YOUNG, K. S. Employee internet misuse: an epidemic in need of a research framework. **Journal of Business and Information Technology**, [S.l.], v.1, n.1, p.30 – 36, 2001.

CESAR, J.; LEITE, S. P.; YU, Y.; LIU, L.; YU, E. S. K.; MYLOPOULOS, J. **Quality-Based Software Reuse**. 2005.

CHEN, J. V.; CHEN, C. C.; YANG, H.-H. An empirical evaluation of key factors contributing to internet abuse in the workplace. **Industrial Management & Data Systems**, [S.l.], v.108, n.1, p.87–106, 2008.

CHOU, C.-H.; SINHA, A. P.; ZHAO, H. A text mining approach to Internet abuse detection. **Information Systems and e-Business Management**, [S.l.], v.6, n.4, p.419–439, jan 2008.

CHOU, C.-H.; SINHA, A. P.; ZHAO, H. Commercial Internet filters: perils and opportunities. **Decision Support Systems**, [S.l.], v.48, n.4, p.521 – 530, 2010.

CHOU, C.-H.; SINHA, A. P.; ZHAO, H. A Hybrid Attribute Selection Approach for Text Classification. **J. AIS**, [S.l.], v.11, n.9, 2010.

CHUN, Z. Y.; BOCK, G.-W. Why Employees Do Non-Work-Related Computing : an investigation of factors affecting nwrc in a workplace. **The Tenth Pacific Asia Conference on Information Systems (PACIS 2006)**, [S.l.], n.Pacis, p.1259–1273, 2006.

COOVERT; GOLDSTEIN. Locus of control as a predictor of users' attitude toward computers. Psychological Reports. **Psychological Reports**, [S.l.], v.47, p.1167–1173, 1980.

Planning, and Developing the Company Organization Structure. 3a.ed. [S.l.]: Americtm Management Association, 1955.

DAVIS, R.; FLETT, G.; BESSER, A. Validation of a new scale for measuring problematic Internet use: implications for pre-employment screening. **CyberPsychology And Behavior**, [S.l.], v.4, p.331 – 345, 2002.

DIEHL, M.; STROEBE, W. Productivity Loss In Brainstorming Groups: toward the solution of a riddle. **Journal of Personality and Social Psychology**, [S.l.], v.53, n.3, 1987.

DOHERTY, N. F.; ANASTASAKIS, L.; FULFORD, H. Reinforcing the security of corporate information resources: a critical review of the role of the acceptable use policy. **International Journal of Information Management**, [S.l.], v.31, n.3, p.201–209, jun 2011.

DOUGLAS, D. E. PERT and simulation. In: WINTER SIMULATION - VOLUME 1, 10., 1978, Piscataway, NJ, USA. **Proceedings...** IEEE Press, 1978. p.89–98. (WSC '78).

FERRAIOLO, D. F.; SANDHU, R.; GAVRILA, S.; KUHN, D. R.; CHANDRAMOULI, R. Proposed NIST standard for role-based access control. **ACM Trans. Inf. Syst. Secur.**, New York, NY, USA, v.4, p.224–274, August 2001.

GALLETTA, D. F.; POLAK, P. An Empirical Investigation of Antecedents of Internet Abuse in the Workplace. **Security**, [S.l.], n.2002, p.47–51, 2003.

GRIFFITHS, M. Internet abuse and internet addiction in the workplace. **Journal of Workplace Learning**, [S.l.], v.22, n.7, p.463–472, 2010.

HELPER, S.; SAKO, M. Management innovation in supply chain: appreciating chandler in the twenty-first century. **Industrial and Corporte Change**, [S.l.], v.19(2), p.399–429, 2010.

KLEIN, K. E. Setting a Realistic Web-Use Policy. **Business Week Online**, [S.l.], v.28, p.18–18, July 2007.

KOLFSCHOTEN, G. Cognitive Load in Collaboration - Brainstorming. In: SYSTEM SCIENCES (HICSS), 2011 44TH HAWAII INTERNATIONAL CONFERENCE ON, 2011. **Anais...** [S.l.: s.n.], 2011. p.1 –9.

The Rational Unified Process: an introduction (3rd edition). 3.ed. [S.l.]: Addison-Wesley Professional, 2003.

LI, H.; ZHANG, J.; SARATHY, R. Understanding compliance with internet use policy from the perspective of rational choice theory. **Decision Support Systems**, [S.l.], v.48, n.4, p.635 – 645, 2010.

LIAO, Q.; LUO, X.; LI, L. WORKPLACE MANAGEMENT AND EMPLOYEE MISUSE: does punishment matter? **The Journal of Computer Information Systems (JCIS)**, [S.l.], v.50, n.2, 2009.

MACEDO, R.; MOZZAQUATRO, B.; NUNES, R. Uma Arquitetura de Segurança para Mecanismos de Controle de Acesso Baseados em Serviços Web. **10ª Simpósio Brasileiro em Segurança da Informação e Sistemas Computacionais**, Fortaleza - CE, 2010.

MACEDO, R.; NUNES, R.; BANDEIRA, J. Modelo de Controle de Acesso Baseado em Expressões Contextuais. **XXXVI Conferência Latino Americana de Informática CLEI**, Assunção - Paraguai, 2010.

MAHANEY, R. C.; LEDERER, A. L. The role of monitoring and shirking in information systems project management. **International Journal of Project Management**, [S.l.], v.28, n.1, p.14–25, jan 2010.

NING, J.; CHEN, Z.; LIU, G. PDCA process application in the continuous improvement of software quality. In: COMPUTER, MECHATRONICS, CONTROL AND ELECTRONIC ENGINEERING (CMCE), 2010 INTERNATIONAL CONFERENCE ON, 2010. **Anais...** [S.l.: s.n.], 2010. v.1, p.61 –65.

NIST. A Survey of Access Control Models. **NIST Privilege (Access) Management Workshop**, [S.l.], 2009.

PANKO, R. R.; BEH, H. G. Monitoring for pornography and sexual harassment. **Commun. ACM**, New York, NY, USA, v.45, p.84–87, January 2002.

PEE, L. G.; WOON, I. M.; KANKANHALLI, A. Explaining non-work-related computing in the workplace: a comparison of alternative models. **Information and Management**, [S.l.], v.45, n.2, p.120 – 130, 2008.

POLLARD, S.; CADSBY, J. Electronic brainstorming, anonymity and Deviance. **School of Business**, Ontario - Canadá, 1996.

PRIEBE, T.; DOBMEIER, W.; KAMPRATH, N. Supporting attribute-based access control with ontologies. In: AVAILABILITY, RELIABILITY AND SECURITY, 2006. ARES 2006. THE FIRST INTERNATIONAL CONFERENCE ON, 2006. **Anais...** [S.l.: s.n.], 2006. p.8 pp.

RAMAYAH, T. Personal web usage and work inefficiency. **Business Strategy Series**, [S.l.], v.11, p.295 – 301, 2010.

RANGEL, E. M. L.; MENDES, I. A. C.; CáRNIO, E. C.; ALVES, L. M. M.; ALMEIDA CRISPIM, J. de; MAZZO, A.; ANDRADE, J. X.; TREVIZAN, M. A.; RANGEL, A. L. Avaliação, por graduandos de enfermagem, de ambiente virtual de aprendizagem para ensino de fisiologia endócrina. **Acta Paul Enferm**, [S.l.], 2011.

RAO, V.; JAEGER, T. Dynamic mandatory access control for multiple stakeholders. In: ACM SYMPOSIUM ON ACCESS CONTROL MODELS AND TECHNOLOGIES, 14., 2009, New York, NY, USA. **Proceedings...** ACM, 2009. p.53–62. (SACMAT '09).

RESTUBOG, S. L. D.; GARCIA, P. R. J. M.; TOLEDANO, L. S.; AMARNANI, R. K.; TOLENTINO, L. R.; TANG, R. L. Yielding to (cyber)-temptation: exploring the buffering role of self-control in the relationship between organizational justice and cyberloafing behavior in the workplace. **Journal of Research in Personality**, [S.l.], v.45, n.2, p.247 – 251, 2011.

SAMARATI, P.; VIMERCATI, S. D. C. d. Access Control: policies, models, and mechanisms. In: REVISED VERSIONS OF LECTURES GIVEN DURING THE IFIP WG 1.7 INTERNATIONAL SCHOOL ON FOUNDATIONS OF SECURITY ANALYSIS AND DESIGN

ON FOUNDATIONS OF SECURITY ANALYSIS AND DESIGN: TUTORIAL LECTURES, 2001, London, UK. **Anais...** Springer-Verlag, 2001. p.137–196.

SANDHU, R.; COYNE, E.; FEINSTEIN, H.; YOUMAN, C. Role-based access control models. **Computer**, [S.l.], v.29, n.2, p.38 –47, feb 1996.

SHARMA, S.; GUPTA, J. Improving workers productivity and reducing internet abuse. **The Journal of Computer Information Systems**, [S.l.], v.44, n.2, 2003.

SIAU, K.; NAH, F. F.-H.; TENG, L. Acceptable internet use policy. **Commun. ACM**, New York, NY, USA, v.45, p.75–79, January 2002.

Metodologia da pesquisa e elaboração de dissertação. [S.l.]: Universidade Federal de Santa Catarina, 2001.

TAN, K. S.; CHONG, S. C.; LIN, B.; EZE, U. C. Internet-based ICT adoption among SMEs: demographic versus benefits, barriers, and adoption intention. **Journal of Enterprise Information Management**, [S.l.], v.23, p.27 – 55, 2010.

TAYLOR, M.; HAGGERTY, J.; GRESTY, D. The legal aspects of corporate computer usage policies. **Computer Law and Security Review**, [S.l.], v.26, n.1, p.72 – 76, 2010.

Interpersonal behavior. [S.l.]: Brooks/Cole Pub. Co., 1977.

VITAK, J.; CROUSE, J.; LAROSE, R. Personal Internet use at work: understanding cyberslacking. **Computers in Human Behavior**, [S.l.], v.In Press, Corrected Proof, p.–, 2011.

WILSON, J. Social networking: the business case - [it internet]. **Engineering Technology**, [S.l.], v.4, n.10, p.54 –56, june 6 2009.

WITTEN, I.; FRANK, E. Data mining practical machine learning tools and techniques, second edition. **Morgan Kaufmann Publishers**, [S.l.], 2005.

YOUNG, K. Policies and procedures to manage employee Internet abuse. **Computers in Human Behavior**, [S.l.], v.26, n.6, p.1467 – 1471, 2010. Online Interactivity: Role of Technology in Behavior Change.

YOUNG, K. S.; CASE, C. J. Internet abuse in the workplace: new trends in risk management. **Cyberpsychology & behavior : the impact of the Internet, multimedia and virtual reality on behavior and society**, [S.l.], v.7, n.1, p.105–11, feb 2004.

YUAN, E.; TONG, J. Attributed based access control (ABAC) for Web services. In: WEB SERVICES, 2005. ICWS 2005. PROCEEDINGS. 2005 IEEE INTERNATIONAL CONFERENCE ON, 2005. **Anais...** [S.l.: s.n.], 2005. p.569.

APÊNDICE A POLÍTICA DE CONTROLE DE ACESSO

```
<?xml version="1.0" encoding="UTF−8"?>
<PolicySet
xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
xmlns:xsi="http://www.w3.org/2001/XMLSchema−instance"
xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os
http://docs.oasis−open.org/xacml/access_control−xacml−2.0−policy−schema−os.xsd"
PolicySetId="urn:va:xacml:2.0:interop:rsa8:policysetid:CDA"
PolicyCombiningAlgId=
"urn:oasis:names:tc:xacml:1.0:policy−combining−algorithm:first−applicable">
    <Description>Politica do Dia X da Semana</Description>
    <Target>
        <Subjects>
            <Subject>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp−string−match">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema
                        string».*</AttributeValue><SubjectAttributeDesignator
                        DataType="http://www.w3.org/2001/XMLSchema string"
                            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject−id"/>
                </SubjectMatch>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchemastring»Ciencia da
                        Computacao</AttributeValue><SubjectAttributeDesignator
                        DataType="http://www.w3.org/2001/XMLSchema string"
                            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:curso"/>
                </SubjectMatch>
                <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
                    <AttributeValue DataType="http://www.w3.org/2001/XMLSchema
                        string»10</AttributeValue><SubjectAttributeDesignator
                        DataType="http://www.w3.org/2001/XMLSchemastring"
                            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:turma"/>
                </SubjectMatch>
            </Subject>
        </Subjects>
    </Target>
    <!−− Disciplina de Tolerancia a Falhas −−>
    <Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema−instance"
        xmlns:context="urn:oasis:names:tc:xacml:1.0:context"
        xmlns:memos="urn:example:documents"
        PolicyId="1"
        RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule−combining−algorithm:permit−overrides">

        <Target>
            <Subjects>
                <Subject>
                    <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
                        <AttributeValue DataType="http://www.w3.org/2001/XMLSchemastring»tolerancia a
                            falhas</AttributeValue><SubjectAttributeDesignator
                            DataType="http://www.w3.org/2001/XMLSchemastring"
                                AttributeId="urn:oasis:names:tc:xacml:1.0:subject:disciplina"/>
                    </SubjectMatch>
                </Subject>
            </Subjects>
            <Resources>
                <Resource>
                    <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
                        <AttributeValue DataType="http://www.w3.org/2001/XMLSchemastring»games-
                            online</AttributeValue><ResourceAttributeDesignator
                            DataType="http://www.w3.org/2001/XMLSchemastring"
                                AttributeId="urn:oasis:names:tc:xacml:1.0:resource:site−class"/>
                    </ResourceMatch>
                </Resource>
            </Resources>
        </Target>

        <Rule RuleId="Periodo1" Effect="Permit">
            <Condition FunctionId="http://research.sun.com/projects/xacml/names/functiontime-in-range»<Apply
                FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only»<EnvironmentAttributeDesignator
                DataType="http://www.w3.org/2001/XMLSchematime"
                    AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current−time"/>
                </Apply>
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema
                    time»07:30:00</AttributeValue><AttributeValue
                    DataType="http://www.w3.org/2001/XMLSchematime">09:20:00</AttributeValue>
            </Condition>
        </Rule>
        <Rule RuleId="Periodo1" Effect="Permit">
            <Condition FunctionId="http://research.sun.com/projects/xacml/names/functiontime-in-range»<Apply
                FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only»<EnvironmentAttributeDesignator
                DataType="http://www.w3.org/2001/XMLSchematime"
                    AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current−time"/>
                </Apply>
                <AttributeValue DataType="http://www.w3.org/2001/XMLSchema
                    time»09:30:00</AttributeValue><AttributeValue
                    DataType="http://www.w3.org/2001/XMLSchematime">12:20:00</AttributeValue>
            </Condition>
        </Rule>
    </Policy>
    <!−− Politica de Redes de Computadores −−>
    <Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema−instance"
        xmlns:context="urn:oasis:names:tc:xacml:1.0:context"
```

```
75          xmlns:memos="urn:example:documents"
76          PolicyId="2"
77          RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule−combining−algorithm:permit−overrides">
78
79          <Target>
80              <Subjects>
81                  <Subject>
82                      <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
83                          <AttributeValue DataType="http://www.w3.org/2001/XMLSchemastring»redes de
                                computadores</AttributeValue><SubjectAttributeDesignator
                                DataType="http://www.w3.org/2001/XMLSchemastring"
84                                      AttributeId="urn:oasis:names:tc:xacml:1.0:subject:disciplina"/>
85                      </SubjectMatch>
86                  </Subject>
87              </Subjects>
88              <Resources>
89                  <Resource>
90                      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
91                          <AttributeValue DataType="http://www.w3.org/2001/XMLSchemastring»games-
                                online</AttributeValue><ResourceAttributeDesignator
                                DataType="http://www.w3.org/2001/XMLSchemastring"
92                                    AttributeId="urn:oasis:names:tc:xacml:1.0:resource:site−class"/>
93                      </ResourceMatch>
94                  </Resource>
95              </Resources>
96          </Target>
97
98          <Rule RuleId="Periodo2" Effect="Permit">
99              <Condition FunctionId="http://research.sun.com/projects/xacml/names/functiontime-in-range»<Apply
                    FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only»<EnvironmentAttributeDesignator
                    DataType="http://www.w3.org/2001/XMLSchematime"
100                                     AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current−time"/>
101                 </Apply>
102                 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema
                        time»08:00:00</AttributeValue><AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchematime">19:30:00</AttributeValue>
103             </Condition>
104         </Rule>
105     </Policy>
106
107 <!−− Politica do Centro −−>
108     <Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
109         xmlns:xsi="http://www.w3.org/2001/XMLSchema−instance"
110         xmlns:context="urn:oasis:names:tc:xacml:1.0:context"
111         xmlns:memos="urn:example:documents"
112         PolicyId="4"
113         RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule−combining−algorithm:permit−overrides">
114
115         <Target>
116             <Subjects>
117                 <Subject>
118                     <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
119                         <AttributeValue DataType="http://www.w3.org/2001/XMLSchema
                                string»aluno</AttributeValue><SubjectAttributeDesignator
                                DataType="http://www.w3.org/2001/XMLSchemastring"
120                                     AttributeId="urn:oasis:names:tc:xacml:1.0:subject:perfil"/>
121                     </SubjectMatch>
122                 </Subject>
123             </Subjects>
124             <Resources>
125                 <Resource>
126                     <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string−equal">
127                         <AttributeValue DataType="http://www.w3.org/2001/XMLSchemastring»games-
                                online</AttributeValue><ResourceAttributeDesignator
                                DataType="http://www.w3.org/2001/XMLSchemastring"
128                                   AttributeId="urn:oasis:names:tc:xacml:1.0:resource:site−class"/>
129                     </ResourceMatch>
130                 </Resource>
131             </Resources>
132         </Target>
133         <Rule RuleId="Periodo1" Effect="Permit">
134             <Condition FunctionId="http://research.sun.com/projects/xacml/names/functiontime-in-range»<Apply
                    FunctionId="urn:oasis:names:tc:xacml:1.0:function:time-one-and-only»<EnvironmentAttributeDesignator
                    DataType="http://www.w3.org/2001/XMLSchematime"
135                                     AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current−time"/>
136                 </Apply>
137                 <AttributeValue DataType="http://www.w3.org/2001/XMLSchema
                        time»13:30:00</AttributeValue><AttributeValue
                        DataType="http://www.w3.org/2001/XMLSchematime">18:00:00</AttributeValue>
138             </Condition>
139         </Rule>
140     </Policy>
141 </PolicySet>
```

Política A.1: Modelo de PCA Utilizado no SGPCA

APÊNDICE B QUESTIONÁRIOS

B.1 Pré-implantação

Prezado(a) Professor(a), Esta pesquisa tem o objetivo de verificar a percepção dos professores a respeito da liberação de uso da Internet via rede sem fio aos alunos do Centro de Tecnologia, bem como a respeito do uso de aspectos dinâmicos no controle de acesso à rede sem fio (políticas de controle de acesso).

O trabalho é parte das atividades de mestrado do acadêmico Ricardo Tombesi Macedo, do Programa de Pós-Graduação em Engenharia de Produção (PPGEP), que está sendo orientado pelo Prof. Raul Ceretta Nunes do Grupo de Pesquisa em Gestão e Tecnologia em Segurança da Informação (GTSeg).

Data: __ / __ / _____

1. Qual o número de disciplinas ministradas por você:

   ☐ Uma.

   ☐ Duas.

   ☐ Três.

   ☐ Quatro.

   ☐ Mais de quatro.

2. As disciplinas ministradas por você predominam-se aspectos:

   ☐ Teóricos.

   ☐ Práticos.

   ☐ Ambos.

3. Você considera importante os alunos acessarem a rede sem fio do CT durante o horário de aula?

   ☐ Sim.

   ☐ Não.

   Que problemas você prevê que podem acontecer?

4. Em sua opinião, que tipo de aula pode se beneficiar mais do uso da Internet:

   ☐ Teórica.

   ☐ Prática.

   ☐ Nenhuma.

5. Você considera importante ter políticas de controle de acesso configuráveis/adaptáveis à suas aulas teóricas e práticas?

   ☐ Sim.

   ☐ Não.

6. Você considera que a utilização de recursos da Web pode potencializar o aprendizado dos conteúdos de sua disciplina?

   ☐ Considera irrelevante.

   ☐ Considera pouco relevante.

   ☐ Considera relevante.

   ☐ Considera muito relevante.

7. Abaixo, marque quais tipos de navegação poderiam contribuir para o aprendizado em suas disciplinas:

   ☐ Redes sociais.

   ☐ Fóruns.

   ☐ Mensagens Instantâneas.

   ☐ Serviço de *e-mail*.

   ☐ Sites de pesquisa.

   ☐ Conteúdos sobre jogos.

   ☐ *Chat*.

   ☐ *Hacking*.

   ☐ Nenhuma.

   ☐ Outros. Quais?

8. Quanto ao intervalo de suas disciplinas com mais de um período, você costuma:

   ☐ Ministrar de forma isolada os períodos de cinqüenta minutos, gerando dois intervalos.

   ☐ Unir os períodos e gerar apenas um intervalo.

9. Você costuma dividir a forma de ministrar os conteúdos de suas disciplinas, tais como: só aulas teóricas ou só aulas práticas, ou outra forma de divisão?

   ☐ Não costuma.

   ☐ Quase nunca divide os conteúdos..

☐ Divide os conteúdos regularmente.

☐ Sempre divide os conteúdos.

10. Considerando aulas teóricas e práticas, você acredita que seus alunos possuiriam necessidade de acesso a recursos da Web diferenciados em cada tipo de aula?

    ☐ Nunca.

    ☐ Quase nunca.

    ☐ Regularmente.

    ☐ Sempre.

11. Nas suas aulas, com que freqüência você costuma aplicar trabalhos, exercícios, atividades práticas ou qualquer prática docente que poderiam ser melhor desempenhadas com auxílio de recursos disponíveis na Web:

    ☐ Nunca.

    ☐ Quase nunca.

    ☐ Regularmente.

    ☐ Sempre.

12. O quanto você considera importante definir políticas de controle de acesso a rede sem fio para os estudantes.

    ☐ Irrelevante..

    ☐ Pouco relevante.

    ☐ Relevante.

    ☐ Muito relevante.

13. Você considera importante o professor da disciplina definir políticas de controle de acesso customizadas que serão aplicadas aos seus alunos somente no horário de sua disciplina?

    ☐ Irrelevante.

    ☐ Pouco relevante.

    ☐ Relevante.

    ☐ Muito relevante.

14. Para suas disciplinas, considerando que os alunos tenham acesso a Internet durante as aulas, o quanto você considera importante atualizar configurações de acesso (que indicam permissões ou não de acesso) e tipos de sites durante o semestre?

☐ Não considera.

☐ Considera pouco.

☐ Considera relevante.

☐ Considera muito relevante.

B.2 Pós-implantação

1. Você considera importante os alunos acessarem a rede sem fio do CT durante o horário de aula?

   ☐ Sim.

   ☐ Não.

   Que problemas você prevê que podem acontecer?

2. Em sua opinião, que tipo de aula pode se beneficiar mais do uso da Internet:

   ☐ Teórica.

   ☐ Prática.

   ☐ Ambas.

   ☐ Nenhuma.

3. Você considera importante ter políticas de controle de acesso configuráveis/adaptáveis à suas aulas teóricas e práticas?

   ☐ Sim.

   ☐ Não.

4. Você considera que a utilização de recursos da Web pode potencializar o aprendizado dos conteúdos de sua disciplina?

   ☐ Considera irrelevante.

   ☐ Considera pouco relevante.

   ☐ Considera relevante.

   ☐ Considera muito relevante.

5. Abaixo, marque quais tipos de navegação poderiam contribuir para o aprendizado em suas disciplinas:

   ☐ Redes sociais.

   ☐ Fóruns.

☐ Mensagens Instantâneas.

☐ Serviço de *e-mail*.

☐ Sites de pesquisa.

☐ Conteúdos sobre jogos.

☐ *Chat*.

☐ *Hacking*.

☐ Nenhuma.

☐ Outros. Quais?

6. Com base nas experiências após a liberação de acessos aos alunos, você sentiu a necessidade de customizar as permissões de acessos à rede sem fio?

7. Em sua opinião, quais mudanças deveriam ser efetuadas no configurador de acessos para melhor servir as necessidades dos professores durante as aulas.

8. O quanto você considera importante definir políticas de controle de acesso a rede sem fio para os estudantes.

   ☐ Irrelevante.

   ☐ Pouco relevante.

   ☐ Relevante.

   ☐ Muito relevante.

9. Você considera importante o professor da disciplina definir políticas de controle de acesso customizadas que serão aplicadas aos seus alunos somente no horário de sua disciplina?

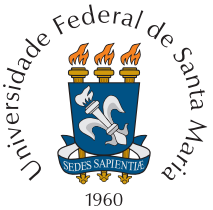
   ☐ Irrelevante.

   ☐ Pouco relevante.

   ☐ Relevante.

   ☐ Muito relevante.

APÊNDICE C POLÍTICA DE UTILIZAÇÃO DA INTERNET



UNIVERSIDADE FEDERAL DE SANTA MARIA

CENTRO DE TECNOLOGIA

Política de Uso da Internet Sem Fio

C.1 Introdução

O **Centro de Tecnologia** (CT) da **Universidade Federal de Santa Maria** (UFSM) tem como prover um serviço de Internet sem fio de qualidade, mantendo o maior nível de segurança e privacidade para seus usuários. Este documento contém diretrizes que regem a política responsável por prover o nível de segurança e privacidade mencionados. De modo que este torna-se um adendo ao contrato de prestação de serviço estabelecido entre o usuário e o CT/UFSM. Para melhor compreensão deste documento, torna-se interessante entender:

- O CT/UFSM configurou seus serviços de Internet sem fio para prover acesso qualificado, visando beneficiar os professores, alunos e funcionários.
- Este documento é projetado para assegurar que todos os usuários possam usar responsavelmente os serviços de Internet sem fio fornecidos pelo CT/UFSM.
- O CT/UFSM pode modificar este documento periodicamente. Sendo que, quando tornar-se necessário, os usuários serão informados ao logar no sistema.
- O termo “usuário"utilizado ao longo do documento é definido como um utilizador dos recursos da rede sem fio. De forma que, este pode ser referenciado mais especificamente como aluno, docente ou técnico-administrativo.

C.2 Serviço

O serviço conta com dois pilares, sendo eles a autenticação e autorização. Sendo que a autenticação apresenta as seguintes particularidades:

- Ao tentar acessar qualquer site através da rede sem fio, o usuário será redirecionado a uma página de login, onde o mesmo deverá autenticar-se. Esta autenticação ocorrerá em modo de segurança, via protocolo HTTPS, por tanto, será exigido ao usuário confirmar uma exceção de segurança quanto ao certificado apresentado. Vale lembrar que este procedimento acontecerá somente na primeira vez que um usuário tentar acessar a rede.

- O usuário e senha utilizado para acessar a rede sem fio corresponde ao mesmo que o do portal do aluno, portal do professor ou biblioteca.

Enquanto que a autorização agrega as seguintes peculiaridades:

- Docentes e técnicos-administrativos possuirão acesso irrestrito à Internet.

- Fora do horário de aula, os alunos deverão ter acessos regidos conforme especificado no capítulo C.4.

- Durante o horário de aula, fica à critério do docente liberar ou não acesso à *Web*. Sendo que para isto, o mesmo terá acesso ao **Sistema de Gestão de Políticas de Controle de Acesso**, disponível em *http://www.gtseg.ufsm.br/configuradorWirelessCt*, para gerir como se dará o acesso à Internet durante suas aulas.

Frisa-se ainda, que toda a navegação dos usuários são confidenciais. No entanto, em caso de descumprimento das diretrizes especificadas no capítulo C.5, essas informações poderão ser objeto de auditoria.

C.3 Responsabilidades

As seguintes responsabilidades são definidas para os usuários:

- O usuário é responsável por sua conta e suas respectiva senhas.
- A única pessoa permitida a usar uma conta é o usuário com matrícula emitida pela UFSM.
- O usuário tem que seguir as orientações dadas pelo administrador do sistema com respeito ao uso dos serviços.
- O usuário tem que usar os recursos da Internet eficazmente.
- Ao marcar a opção “aceito os termos de uso"automaticamente o usuário consente com as diretrizes deste documento.

C.4 Uso Autorizado

O Centro de Tecnologia permite ao usuário:

- Acessar páginas da Internet voltadas à missão do CT/UFSM, que é “promover ensino, pesquisa e extensão, formando lideranças capazes de auxiliar no desenvolvimento da sociedade".
- Acessar Sites de Pesquisa, Fóruns e Serviço de e-mail durante as aulas, se permitido pelo docente.

C.5 Uso Desautorizado

Não será permitido ao usuário:

- Copiar, transferir, examinar, alterar ou excluir qualquer informação pertencente a outros usuários.
- Interferir nos sistemas responsáveis pela administração da Internet.
- Armazenar, transmitir, ou receber qualquer material de conteúdo obsceno, de natureza repetitiva, ou ilegal.
- Utilizar a Internet sem fio para obter acesso não autorizado em qualquer computador ou serviço.
- Copiar qualquer dado, software, música, ou filme da Internet protegido por direitos autorais, a menos que autorizado pelo dono.
- Fazer qualquer tentativa para descobrir conta ou senha de outros usuários, ou para serviços os quais o acesso não foi autorizado.
- Enviar *e-mail* de caráter não acadêmico ou profissional para os demais usuários.
- Acessar páginas relacionadas a sexo explicito, habilidades criminais, jogos *on-line*, entretenimento *on-line*.
- Congestionar a rede devido a tráfego impróprio.
- Utilizar a Internet de maneira improdutiva.

C.6 Atividades Disciplinares

Caso um usuário realize alguma das atividades não permitidas especificadas no capítulo C.5, ou apresente conduta considerada prejudicial através da perspectiva dos interesses do CT/UFSM, a administração do centro pode aplicar as seguintes medidas:

- Suspender o usuário do uso da Internet por um período especificado.
- Cancelar o acesso do usuário à Internet.
- Realizar indicações às autoridades legais.
- Relatar o fato ocorrido para que seja feito acompanhamento ético-profissional ou abertura de processo disciplinar.

C.7 Considerações Finais

O CT/UFSM não é responsável pelo conteúdo de material obtido pela Internet. Também não se responsabiliza pelos possíveis danos causados pelos usuários, que tendo acesso à Internet, obtiverem qualquer material de natureza ofensiva, inclusive material que descreve material de natureza ofensiva, com conteúdos de sexo explicito, violência ou habilidades criminais.

Em caso de uso indevido da senha de acesso por terceiros, favor entrar em contato imediatamente com o Centro de Processamento de Dados para realizar a troca de senha.

O login de acesso à rede sem fio só terá validade enquanto perdurar o vínculo do aluno, técnico-administrativo, ou docente com a instituição.

A configuração do equipamento de acesso será de responsabilidade do usuário, liberando o CT/UFSM de qualquer ônus de configuração dos dispositivos de acesso.

APÊNDICE D PLANO DE ENSINO

PLANO DE ENSINO

Curso, Habilitação: Ciência da Computação

Disciplina: Banco de Dados II Período: 7°

Créditos: 04 Horas-aula: 60 Semestre Letivo: 2011 - 2

Professor: Daniel Pezzi da Cunha Horário: 19:00 às 22:30

Perfil do egresso:

Com os conhecimentos adquiridos durante o Curso de Ciência da Computação e empregando recursos tecnológicos modernos, o egresso deverá apresentar as seguintes aptidões (seja atuando na área acadêmica ou na empresarial):

- Pesquisar soluções e criar novos processos e tecnologias para as necessidades detectadas;
- Questionar a realidade, formulando problemas e tratando de resolvê-los, utilizando, para isso, o pensamento lógico, a criatividade, a intuição, a capacidade de análise crítica, selecionando procedimentos e verificando sua adequação;
- Participar de trabalhos em equipe, organizando e realizando tarefas no processo de desenvolvimento de sistemas computacionais;
- Em conjunto com outros profissionais, resolver problemas computacionais de qualquer natureza;
- Gerenciar e administrar a implantação de novas tecnologias;
- Acompanhar, treinar e gerenciar o uso dos recursos de informática;
- Analisar sistemas de software;
- Assessorar usuários na escolha e uso de programas e sistemas de software ;
- Definir métodos, ferramentas e procedimentos de apoio ao desenvolvimento de software;
- Desenvolver e gerenciar projetos de sistemas de software;
- Criar, planejar e desenvolver Sistemas de Informação;
- Implantar e garantir normas de segurança de dados, equipamentos e sistemas computacionais;
- Disposição para um estado permanente de estudo de novos e complexos assuntos.

Ementa:

Conceitos avançados sobre banco de dados; Arquiteturas de sistemas de banco de dados não convencionais; Técnicas de controle de concorrência; Mecanismos de recuperação de dados.

Objetivos da disciplina:

Proporcionar o estudo e o conhecimento avançado de bancos de dados, tornando o acadêmico apto a avaliar os mecanismos de gerenciamento interno de SGBDs e de processamento de

transações, administrar diferentes tipos de bancos de dados, descrever e analisar os principais protocolos de controle de concorrência e ser capaz de definir estratégias de recuperação de dados.

Conteúdo programático:

- Revisão de operações DDL e DML em linguagem SQL;
- Processamento de consultas: medidas de custo de uma consulta, avaliação de expressões e otimizações.
- Indexação e hashing: índices ordenados, arquivos de índice Árvore-B, Hashing Estático e Dinâmico e índice em SQL.
- Transações: estados, implementação de atomicidade e durabilidade, execuções concorrentes, serialização e recuperação.
- Controle de concorrência: protocolos baseados em Bloqueios, Timestamp, Validação, Granularidade Múltipla, Esquemas Multiversão e Manuseio de Deadlock.
- Sistema de recuperação: recuperação baseada em log, Paginação Shadow e gerenciamento de buffer.
- Bancos de dados distribuídos: armazenamento distribuído de dados, transparência de rede, consultas distribuídas, tratamento de impasses e sistemas de múltiplos bancos de dados.
- Bancos de Dados Orientados a Objetos: o modelo orientado a objetos, linguagens O.O., linguagens de programação persistentes e sistemas relacionais-objeto;
- Aplicações especiais: sistemas de suporte a decisão, Data Mining, Data Warehousing, B.D. espaciais, B.D. geográficos, B.D. multimídia e B.D. móveis e pervasivos.

Metodologia e suas estratégias:

As aulas serão baseadas em uma abordagem dialética, priorizando: o desenvolvimento da consciência crítica, a autonomia, o processo reflexivo e a produção do conhecimento. Como estratégias, serão utilizadas os seguintes instrumentos:

- Explanação oral do conteúdo teórico;
- Exercícios envolvendo o conteúdo de cada aula;
- Debate sobre as soluções dos exercícios da aula;
- Provas teóricas descritivas;
- Atividades práticas em laboratório;
- Projeto e desenvolvimento prático de uma base de dados distribuída.

Avaliação:

A avaliação será contínua e processual, tendo como: Critérios:

- A capacidade de entendimento, interpretação e argumentação do conteúdo;
- O comportamento responsável, participativo e crítico.

Instrumentos: Serão aplicados três tipos de avaliações, sendo: provas teóricas descritivas, debates sobre as soluções dos exercícios e artigos resumidos. A média final será calculada da seguinte forma: (Bimestre 1 + Bimestre 2) / 2

- Bimestre 1
  - Prova teórica descritiva = 5,0
  - Respostas dos exercícios = 2,0
  - Desenvolvimento prático de uma base de dados distribuída = 3,0
- Bimestre 2
  - Prova teórica descritiva = 5,0
  - Respostas dos exercícios = 2,0
  - Desenvolvimento prático de uma base de dados distribuída = 3,0

Bibliografia Básica:

ELMASRI, Ramez; NAVATHE, Shamkant B. Sistemas de Banco de Dados. 4.ed. São Paulo: Addison Wesley, 2006.

HEUSER, Carlos Alberto. Projeto de Banco de Dados. 4 ed. Porto Alegre: Sagra Luzzatto, 2001. SILBERSCHATZ, Abrahan; KORTH, Henry F. and SUDARSHAN, S. Sistemas de Banco de Dados. 3 ed. São Paulo: Makron Books, 1999.

Bibliografia Complementar:

DATE, C. J. Introdução à sistemas de banco de dados. 4 edição. Rio de Janeiro: Campus, 2000.

FREEMAN, Robert. Oracle - Referência para o DBA. São Paulo: Elsevier, 2005 GARCIA - MOLINA, Hector; ULLMAN, Jeffrey D.; WIDOM, Jennifer. Implementação de Sistemas de Bancos de Dados. São Paulo: Campus, 2001.

GUTTA, Rajendra. Oracle DBA Automation Scripts. Estados Unidos: SAMS, 2002. HARRINGTON, Jan L. Projetos de bancos de dados relacionais. Rio de Campus: Campus, 2002.

HERNANDEZ, Michael J. Aprenda a projetar seu próprio banco de dados. São Paulo: Makron Books, 2000.

LARMAN, Craig. Utilizando UML e Padrões: Uma introdução à análise e ao projeto orientados a objetos. Porto Alegre: Bookman, 2000.

MANZANO, José Augusto N. G. Estudo dirigido: SQL. São Paulo: Érica, 2002. MOLINA, Hector Garcia. Implementação de Sistemas de Bancos de Dados. Rio de Janeiro: Ed. Campus, 2001.

NEVES, Denise Lemes Fernandes. PostgreSQL : conceitos e aplicações. São Paulo: Érica, 2002.

ÖZSU, M. Tamer; VALDURIEZ, Patrick. Princípios de sistemas de bancos de dados distribuídos. Rio de Janeiro: Campus, 2001.

RAMALHO, José Antonio Alves. SQL: a linguagem dos bancos de dados. São Paulo: Berkeley, 1999.

REESE, George. JDBC e Java: Programação para Banco de Dados. 2.ed. São Paulo: Berkeley, 2001. SILBERSCHATZ, Abraham; KORTH, Henry F.; SUDARSHAN, S. Sistema de Banco de Dados. 5ª ed. São Paulo: Campus, 2006.

Cruz Alta - RS, 25 de agosto de 2011.

ANEXO 2 - DESCRIÇÃO DO TRABALHO EM GRUPO

DESENVOLVIMENTO PRÁTICO

Descrição: desenvolver uma base de dados distribuídos utilizando o PostgreSQL (PostgreSQL Global Development Group).

Componentes: no máximo 2 acadêmicos.

Entrega: as etapas descritas abaixo devem ser mostradas ao professor até o dia 13/10/2011.

Etapas:

- Projeto conceitual e lógico de uma base dados; (0,5)
- Configuração de chaves e índices. (0,5)
- Configuração de gatilhos diversos. (0,5)
- Configuração de Procedimentos Armazenados com operações de inserção, remoção e atualização de dados. (0,5)
- Configuração de visões com variados tipos de consultas. (0,5)
- Configuração de usuários com diversos níveis de acesso. (0,5)

Recomendações:

- Não serão aceitos trabalhos entregues fora da data especificada e sem as devidas identificações.
- Cópias parciais ou completas de outros trabalhos resultarão em invalidação da pesquisa, implicando em nota ZERO.

ANEXO 3 - DESCRIÇÃO DO TRABALHO EM GRUPO

DESENVOLVIMENTO PRÁTICO

Descrição: desenvolver uma base de dados distribuídos utilizando o PostgreSQL (PostgreSQL Global Development Group).

Componentes: no máximo 2 acadêmicos.

Entrega: as etapas descritas abaixo devem ser mostradas ao professor até o dia 08/12/2011.

Etapas:

- Configuração de técnicas de recuperação de dados. (1,0)
- Desenvolvimento de um sistema de suporte a decisão. (1,0)
- Desenvolvimento em banco de dados não convencionais. (1,0)

Recomendações:

- Não serão aceitos trabalhos entregues fora da data especificada e sem as devidas identificações.
- Cópias parciais ou completas de outros trabalhos resultarão em invalidação da pesquisa, implicando em nota ZERO.

Tabela D.1: Cronograma de Trabalho

Data	Assunto	Atividades e estratégias
25/08/2011	Explanação sobre cada tópico do Plano de Ensino; Revisão de operações DDL e DML em linguagem SQL; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula.
01/09/2011	Estudo de caso Firebird; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula; Debate sobre as soluções dos exercícios.
08/09/2011	Processamento de consultas: medidas de custo de uma consulta, avaliação de expressões, otimizações; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula.
15/09/2011	Estudo de caso PostgreSQL; Indexação e hashing: índices ordenados, arquivos de índice Árvore-B, Hashing Estático e Dinâmico, índice em SQL; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula; Debate sobre as soluções dos exercícios.
22/09/2011	Transações: estados, implementação de atomicidade e durabilidade, execuções concorrentes, serialização, recuperação; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula.
29/09/2011	Controle de concorrência: protocolos baseados em Bloqueios, Timestamp e Validação; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula; Debate sobre as soluções dos exercícios.
06/10/2011	Granularidade Múltipla, Esquemas Multiversão, Manuseio de Deadlock; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula; Debate sobre as soluções dos exercícios.
13/10/2011	1ª prova teórica	Prova teórica descritiva
15/10/2011	Seminário Interdisciplinar	
20/10/2011	Análise das questões da prova; Sistema de recuperação: recuperação baseada em log, Paginação Shadow, gerenciamento de buffer; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula.
27/10/2011	Bancos de dados distribuídos: armazenamento distribuído de dados, transparência de rede, consultas distribuídas; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula; Debate sobre as soluções dos exercícios.
03/11/2011	Tratamento de impasses, sistemas de múltiplos bancos de dados; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula.
10/11/2011	Bancos de Dados Orientados a Objetos: o modelo orientado a objetos, linguagens O.O., linguagens de programação persistentes, Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula; Debate sobre as soluções dos exercícios.
17/11/2011	Sistemas relacionais-objeto; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula.
24/11/2011	Aplicações especiais: sistemas de suporte a decisão, Data Mining, Data Warehousing; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula; Debate sobre as soluções dos exercícios.
01/12/2011	B.D. espaciais, B.D. geográficos, B.D. multimídia, B.D. móveis e pervasivos; Exercícios de fixação.	Explanação oral do conteúdo teórico; Exercícios envolvendo o conteúdo da aula.
08/12/2011	2ª prova teórica	Prova teórica descritiva.
15/12/2011	Exame	Prova teórica descritiva.

APÊNDICE E ORGANOGRAMA HIERÁRQUICO DA UFSM

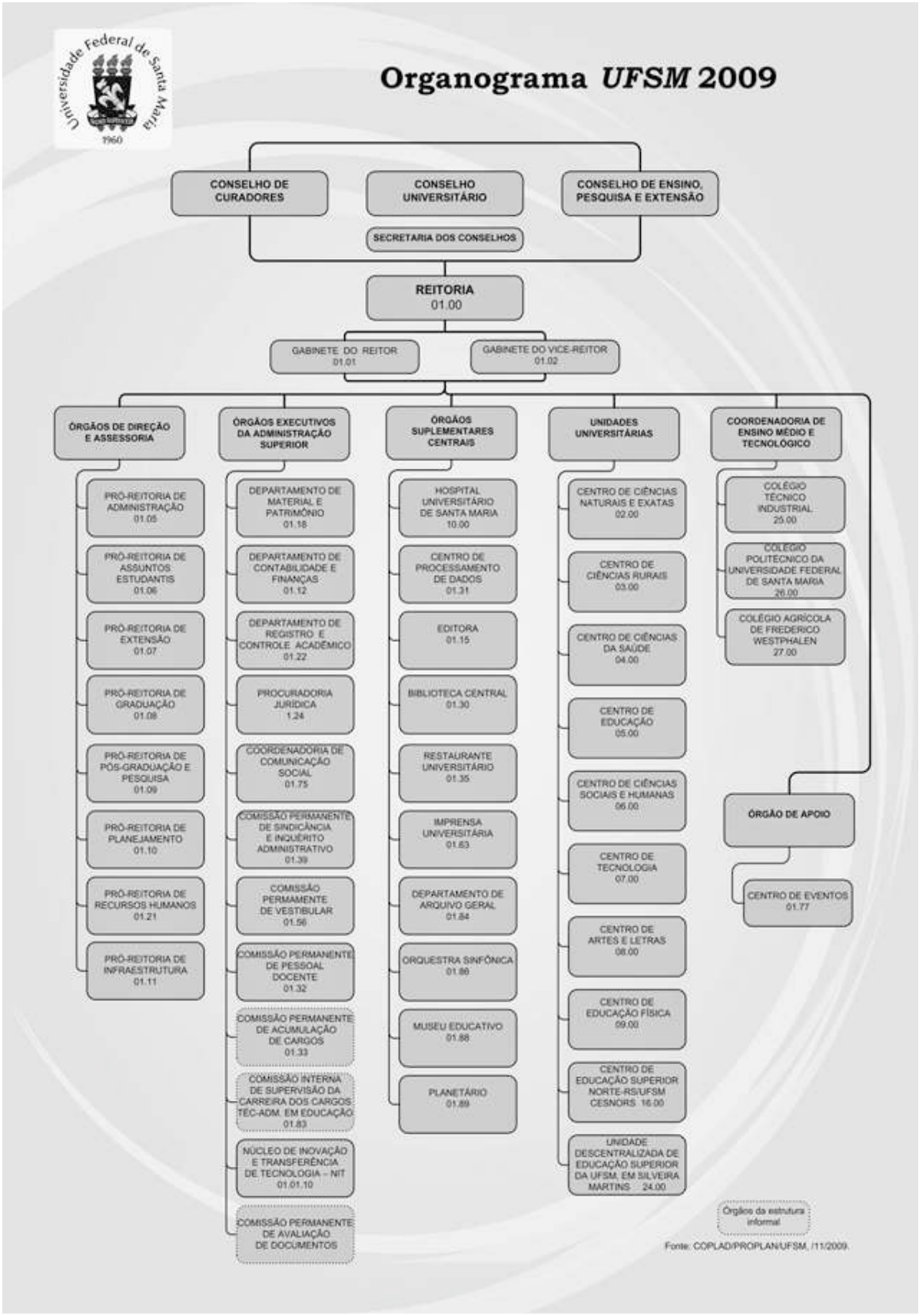


Figura E.1: Organograma Hierárquico da UFSM