POLÍTICA DE SEGURANÇA DA INFORMAÇÃO APLICADA EM UMA INSTITUIÇÃO DE ENSINO MEDIANTE ANÁLISE DE RISCO

Sérgio Duque Castilho[1]; Miguel Feitoza da Fonte[2]

Resumo
Com o crescimento da tecnologia dentro das empresas, tornando-as cada vez mais conectadas com o mundo para buscar ou trocar informações, tornou-se necessário o aumento da sua proteção. Segundo a NBR ISO/IEC 27002, que recomenda as melhores práticas de Segurança da Informação estabeleceu-se que a informação é um ativo que deve ser protegido, como qualquer outro, pois é importante e essencial para os negócios de uma organização. A partir desses conceitos, foi desenvolvido este trabalho com o objetivo de propor uma Política de Segurança da Informação para ser utilizada nas áreas de trabalho e na rede sem fio de uma instituição de ensino superior. Uma análise de risco realizada através de uma pesquisa quantitativa, identificando os pontos fracos e falhos da rede, serviu para estabelecer algumas das normas da política. Também foi avaliado o nível de satisfação e os principais causadores da lentidão no tráfego da rede. A política de segurança proposta tem a finalidade de diminuir os problemas identificados na pesquisa e proteger os ativos da instituição estipulando normas a serem seguidas de modo a inibir o desperdício dos recursos da rede por usuários não autorizados, padronizando seu uso e procurando diminuir sua lentidão.
Palavras-chave: Informação, Política de Segurança, Segurança da Informação.

INFORMATION SECURITY POLICY APPLIED IN AN EDUCATIONAL INSTITUTION THROUGH RISK ANALYSIS

Abstract
An enforcement in protection has become necessary because of the growth of technology within companies, making them increasingly connected to the world in order to seek or exchange information. According to ISO / IEC 27002 that recommends best practices for Information Security it is established that information is an asset that must be protected like any other, because it is important and essential for businesses organization. This study was developed based on these concepts with the objective of proposing an Information Security Policy that could be used in work areas and wireless network of a graduation institution. A risk analysis study conducted through a quantitative research, identifying weaknesses and faulty network, established some policies. It was also evaluated the level of satisfaction and the main causes of slow network traffic. The Security Policy proposed in this study aims to reduce the problems identified in the survey and to protect the assets of the institution stipulating norms to be followed in order to inhibit the waste of network resources by unauthorized users, and standardize its use to try reduce its slowness .
Keywords: Information, Information Security, Security Policy.

[1] Professor da Faculdade de Tecnologias de Ourinhos FATEC; e-mail: sergiocastilho@uol.com.br.
[2] Graduando em Análise e Desenvolvimento de Sistemas pela Faculdade de Tecnologias de Ourinhos; e-mail: miguel_feitoza_fonte@hotmail.com

1 INTRODUÇÃO

A informação é o elemento básico para que a evolução aconteça e o desenvolvimento humano se realize de forma plena e completa. Segundo Coury (2001), Ward et all (1990) a informação é classificada como um dos recursos cuja gestão mais influencia o sucesso de uma organização. Portanto, com o crescimento das corporações há a dependência de uma estrutura de Tecnologia da Informação e Comunicação (TIC) para seu desenvolvimento. Este conceito é reforçado por Stoner (1999), pois segundo esta autora, somente com informações precisas disponíveis, os administradores podem monitorar o progresso na direção de seus objetivos e transformar os planos em realidade.

A disponibilização da informação utilizando como ferramenta a rede mundial de computadores aumenta as ameaças que exploram as vulnerabilidades e podem causar prejuízos consideráveis para a organização. Neste sentido, uma Política de Segurança da Informação, (PSI), é fundamental para padronizar a utilização de recursos e minimizar os prejuízos, protegendo adequadamente seus ativos (GABBAY, 2003).

Para Finne (1998), risco é a soma das ameaças, das vulnerabilidades e dos valores dos ativos, afirmando ainda que o crescimento de qualquer um destes fatores leva a um crescimento do risco.

O propósito básico da informação, dentro do contexto organizacional, de acordo com Oliveira (1998), é o de habilitar a empresa a alcançar seus objetivos por meio do uso eficiente dos recursos disponíveis (pessoas, materiais, equipamentos, tecnologia, investimento, além da própria informação). Com a afirmação de Oliveira pode-se compreender a premência da disponibilidade da informação dentro de uma organização e a necessidade de estabelecer normas para seu acesso.

A PSI é um conjunto de normas, métodos e procedimentos que devem ser formalizados e divulgados para todos os usuários de forma clara e concisa, para que não haja dúvidas segundo a NBR ISO/IEC 27002. Muitas empresas pecam por não terem uma norma estabelecida de utilização de seus recursos, o que acaba causando incidentes indesejáveis.

A NBR ISO/IEC 27002, é uma norma de sistemas de gestão da segurança da informação, onde podem ser encontradas as melhores práticas para elaborar de modo correto uma PSI. Livros, artigos e sites especializados na área Segurança da Informação (SI) serão utilizados nesta pesquisa que tem como objetivo realizar uma análise de risco através de uma pesquisa quantitativa com os alunos e colaboradores da instituição de ensino superior e propor

uma PSI para ser utilizada nos laboratórios de informática e na rede sem fio de uma instituição de ensino superior.

2 IMPORTÂNCIA DA INFORMAÇÃO

Informação é um conjunto de dados que representa um ponto de vista. Um dado processado é o que gera uma informação segundo a ISO/IEC 27002. Um dado não tem valor antes de ser processado. A partir do seu processamento, ele passa a ser considerado uma informação, que pode gerar conhecimento. Uma mensagem criptografada sem sua chave não tem valor, pois não há a possibilidade de compreendê-la.

Informação é poder segundo Campos (2008), assim, quem possui a informações mais valiosas, é quem está mais amparado e favorecido. Organizações investem cada vez mais em tecnologia para terem destaque ante seus concorrentes, pois o investimento nesta área resulta em segurança ao seu patrimônio e inovação para a satisfação dos seus clientes, resultando em mais lucro para a organização.

Essa disputa pela informação pode ser bem entendida se lembrados os confrontos que alimentaram a Guerra Fria, em que os Estados Unidos e a antiga União Soviética disputavam indiretamente a hegemonia política, economia e militar. Foi uma das épocas mais marcantes no desenvolvimento tecnológico mundial, pois as duas potências mundiais estavam sedentas por informação para se posicionarem a frente uma da outra. Acontecia uma batalha por melhoria em artigos bélicos e conhecimento, em que se melhoravam os equipamentos a fim de manter a soberania perante a outra nação. Essa disputa de conhecimentos e informações foi contribuindo para o desenvolvimento tecnológico mundial como um todo (GUIMARÃES, 2002).

Isto evidencia a importância que carrega a Informação. Segundo a ISO/IEC 27002, a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização, visando a necessidade de ser adequadamente protegida. Como um resultado desse incrível aumento tecnológico, a informação está agora exposta a um crescente número e variedades de ameaças. Sem dúvida a informação é um gerador de capital, e também, muitas vezes vale muito dinheiro. Um exemplo simples é supor que um site de vendas fique indisponível por um dia, ou pelo menos por 8 horas, com isso já é possível identificar a quantidade de produtos não vendidos e o total dos prejuízos diretos, sem mencionar tamanha a insatisfação dos clientes, que não estariam sendo incentivados a uma

futura compra naquele site, o que caracteriza-se em prejuízo indireto. Seria um impacto lastimável que poderia comprometer muito os orçamentos da organização.

Wiener (1954) informa que os homens e os grupos humanos, só absorvem a informação de que sentem necessidade e esteja acessível. Nessa afirmação, Wiener (1954) explica que é da natureza do homem querer aprender apenas o que lhe parece necessário, aquilo que visa utilizar, que porá em prática e também o que tem a capacidade de compreender. Isso é caracterizado pela psicologia como um comportamento que distingue cada um, tornando-nos seres únicos, com identificações diferentes. Logo os assuntos e fatos que se assemelham às identificações são mais absorvidos com mais facilidade do que os outros.

Pignatari (2002) aponta que não é a quantidade de informação emitida que é importante para a ação, mas sim a quantidade de informação capaz de penetrar o suficiente num dispositivo de armazenamento e comunicação, de modo a servir como propulsor para a ação. Essa descrição pode ser entendida se comparada a uma engenharia social, em que uma pessoa não tem em mente a real importância de certa informação e pode deixá-la escapar por descuido. Um gerente pode ser alvo de uma engenharia social de um funcionário mal intencionado.

Em um de seus pensamentos Wiener (1954), faz uma comparação entre mensagem e organismo, onde o organismo se opõe ao caos, à desintegração, à morte, como a mensagem ao ruído. Assim como um organismo precisa de proteção para não se desintegrar, uma informação também precisa ser zelada para que não seja corrompida, extraviada ou mesmo roubada. É aí que entram os procedimentos e as normas a serem seguidas para zelar pela informação e os ativos dentro de uma organização, que são as chamadas PSI.

3 SEGURANÇA DA INFORMAÇÃO

Segundo Nakamura e Geus (2002), a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Isto é especialmente importante no ambiente dos negócios, cada vez mais interconectados. Como um resultado deste incrível aumento da interconectividade, a informação, hoje, está exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades. Essas afirmações levam a necessidade da SI.

Onde estão armazenados dados pessoais, como senhas, movimentação de capital e os dados dos clientes, essa extrema necessidade de sigilo da informação, exige-se uma segurança mais eficaz.

3.1 A necessidade da segurança da informação

Segundo a NBR ISO/IEC 27002 a informação pode existir em diversos meios. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou dita em conversas. Seja qual for o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela sempre receba uma proteção adequada. A NBR ISO/IEC 27001 recomenda que o backup dos sistemas seja armazenado em outro local, o mais longe possível do ambiente atual. O maior exemplo e um dos maiores erros cometidos em questão de ambientes seguros para backups foi o atentado de 11 de setembro, onde foram derrubas as Torres Gêmeas nos EUA. Empresas localizadas na torre A tinham seus backups na torre B. Depois da queda das duas torres, algumas empresas simplesmente sumiram, deixaram de existir. Um erro que poderia ser contornado caso o backup estivesse localizado em outro lado da cidade, ou até distribuídos em outras cidades.

A SI é a sua proteção contra os diversos tipos de ameaças para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades de negócio (NBR ISO/IEC 27002, 2011).

Lyra (2008), afirma que a SI é obtida a partir da implementação de um conjunto de controles adequados incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles, além de implementados, precisam ser estabelecidos, monitorados, analisados criticamente e melhorados onde necessário, para garantir que os objetivos do negócio e da segurança da organização sejam atendidos. Para a implementação de um controle de acesso eficaz será analisado o ativo a ser protegido. Quanto mais importante e de maior valor, maior a quantia investida na sua segurança. Câmeras filmadoras e sistemas biométricos não são equipamentos muito baratos e precisam de profissionais para instalá-los e monitorá-los. É bom apontar que todo tipo de tecnologia é momentânea e é indispensável a atualização e aperfeiçoamento constantes.

3.2 Política de Segurança da Informação

A PSI é um conjunto de normas, métodos e procedimentos que devem ser formalizados e divulgados para todos os usuários de forma clara e concisa, para que não gere dúvida segundo a ISO/IEC 27002.

É basicamente um plano que descreve todos os ativos da empresa, e como eles devem ser protegidos, tendo como objetivo proporcionar para aos usuários as maneiras aceitáveis de

uso, relatando o que é permitido e o que não é. Para a utilização desse documento é necessário a aprovação e conscientização da direção e dos demais departamentos principalmente a gerência de TI para seu andamento.

Uma PSI deve ser analisada por um gestor responsável e capacitado para isso, focando na qualidade de serviço.

Nessa pesquisa foi tomado como base o guia prático para elaboração e implementação da PSI de Ferreira e Araújo (2008).

3.3 Importância da Política

Segundo Danchev (2001), uma PSI fornece as bases para a implementação bem sucedida em projetos relacionados no futuro. Este é sem dúvida a primeira medida que deve ser tomada para reduzir o risco de uso de qualquer recurso de informação da empresa. Nesta afirmação Danchev (2001) relata a importância da informação para a organização, é nada mais do que o combustível para o seu crescimento. O primeiro passo para a segurança dessa informação é a implantação de uma política a ser seguida por todos os colaboradores e usuários. Além de tudo isso a PSI também irá ajudar a definir os ativos críticos de uma empresa, como eles devem ser protegidos e como devem ser utilizados.

3.4 Desenvolvimento da Política

Na elaboração da política e dos procedimentos de SI é imprescindível uma pesquisa sobre melhores práticas em segurança utilizadas no mercado, padrões para discussão com a alta administração, a necessidade de metas da organização e a formalização dos procedimentos para integrá-los às políticas corporativas.

O desenvolvimento e a implantação podem ser divididos em quatro fases segundo Ferreira e Araújo (2008): levantamento das informações, desenvolvimento do conteúdo político e das normas, elaboração dos procedimentos de SI e revisão, aprovação e implementação.

No levantamento das informações, é necessário a obtenção dos padrões, normas e procedimentos já existentes para análise, entendimento das necessidades e uso dos recursos tecnológicos nos processos de negócio. Quando estas não existem, a obtenção de informação sobre os ambientes de negócios como: processos de negócios, tendências de mercado e

controles, áreas de risco, ambiente tecnológico, workflow entre ambientes, redes e plataformas devem ser realizado.

No desenvolvimento do conteúdo da PS o gerenciamento da versão e manutenção da política, deve referenciar-se às políticas já existentes ou de versões anteriores. A atribuição de regras e responsabilidades é feita pelo comitê de SI em conjunto com o proprietário das informações, área de armazenamento, usuários da informação, RH, auditoria interna entre outros. Os critérios para classificação da informação é formado pelos níveis de classificação, reclassificação, armazenamento e descarte.

Os procedimentos de SI e Gerenciamento de Incidentes de Segurança da Informação envolvem vários processos: disciplinar; aquisição e uso de hardware e software; proteção contra software malicioso; segurança e tratamento de mídias; uso de recursos da rede; uso de e-mail; utilização dos recursos de TI; cópias de segurança; manutenção de teste e equipamentos; coleta e registro de falhas; gerenciamento e controle da rede; monitoramento do uso e acesso aos sistemas; uso de controles de criptografia e gerenciamento de chaves; controle de mudança de sistema operacional; inventário dos ativos de informação; controle de acesso físico às áreas sensíveis; segurança física, supervisão de visitantes e prestadores de serviço.

Na fase de Revisão, Aprovação e Implantação das Políticas, Normas e Procedimentos de Segurança da Informação é necessário uma revisão e aprovação das políticas, normas e procedimentos de segurança da informação. A efetiva implementação das políticas, normas e procedimentos de SI por meio de algumas iniciativas como a atuação junto à área responsável pela comunicação, ou áreas correspondente, na orientação para preparação do material promocional de divulgação e de consulta, divulgação das responsabilidades dos colaboradores, a importância das políticas, procedimentos de SI, realização de palestras executivas referentes às políticas e procedimentos desenvolvidos, tendo por público-alvo a presidência, diretoria e gerência se faz necessária. A realização de palestras referentes às políticas, normas e procedimentos de segurança, tendo por público-alvo todos os colaboradores da organização deve ser realizada em seguida.

3.5 Fatores comuns

Alguns fatores são comuns entre políticas bem elaboradas, algumas políticas são mais severas e outras menos severas, mas quase todas seguem os seguintes aspectos segundo Ferreira e Araújo (2008): especificação da política, declaração da alta administração, autores e

patrocinadores da política, referências a outras políticas, normas e procedimentos, procedimentos para requisição de exceções à política, procedimentos para mudanças da política, datas de publicação, validade e revisão.

3.6 Pontos críticos para o sucesso

Ferreira e Araújo (2008), afirmam que para o sucesso de uma PSI alguns itens de vital importância devem ser relacionados. São eles: formalização dos processos e instruções de trabalho; utilização de tecnologias capazes de prover segurança; atribuição formal das responsabilidades e das respectivas personalidades; classificação das informações; treinamento e conscientização constantes.

3.7 Características e benefícios

Para que a política seja efetiva, ela deve ter algumas características como cita Ferreira e Araújo (2008), tais como: ser verdadeira, ser complementada com disponibilidade de recursos, ser válida para todos, ser de simples entendimento e comprometimento da alta administração da organização. Os principais benefícios são divididos em curto, médio e longo prazo.

Os de curto prazo são as formalizações e documentações dos procedimentos de segurança adotados pela organização, implementação de novos procedimentos e controles, prevenção de acessos não autorizados, danos ou interferências no andamento dos negócios, mesmo nos casos de falhas ou desastres e maior segurança nos processos de negócio.

Os de médio prazo são as padronizações dos procedimentos de segurança incorporados na rotina da empresa, adaptação segura de novos processos de negócios, qualificação e quantificação dos sistemas de resposta a incidentes e conformidade com os padrões de segurança ISO\IEC 27002.

Os de longo prazo são os retornos sobre os investimentos realizados por meio da redução de problemas, incidentes e consolidação da imagem corporativa associada à SI.

4 ANÁLISE DE RISCO E ESTADO ATUAL DA REDE

Nesse capítulo serão apontados os problemas observados nos laboratórios de informática e na rede sem fio de uma instituição de ensino superior. Através de uma pesquisa elaborada com o objetivo de avaliar o grau de satisfação dos usuários, podem ser observados

alguns dos pontos que estão colaborando para aumentar e agravar o problema da lentidão da rede cabeada nos laboratórios e na rede sem fio.

4.1 Avaliação da satisfação dos usuários

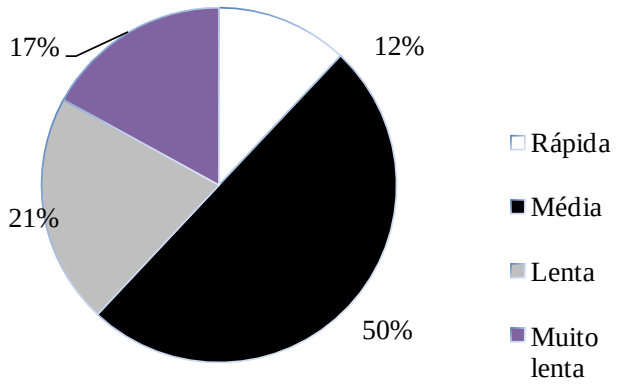
Foi realizada uma pesquisa para a avaliação do desempenho da rede local, o grau de satisfação dos usuários na instituição, o conhecimento e os incidentes em SI. A intenção é saber se os usuários fazem download de dados na instituição, o que pode ser um dos principais fatores que colabora com a lentidão da rede, pois um download pode roubar uma boa quantidade de banda de transmissão de dados, deixando o tráfego muito lento.

Da mesma forma foi avaliado o grau de conhecimento dos usuários em relação à SI para que possa ser comparado com uma Pesquisa Nacional de Segurança da Informação feita pela Módulo (2006). Esse grau de conhecimento é diretamente proporcional ao número de incidentes. Saber se o usuário tem acesso a redes sociais e sites com exibição de filmes dentro da instituição é um dos principais pontos, pois essa também pode ser uma das causas da lentidão da rede.

5 RESULTADOS DA PESQUISA

Serão apresentados alguns dos resultados da pesquisa realizada com cem usuários de uma instituição de ensino superior no período noturno, período com o maior número de acessos e com a maioria dos cursos disponibilizados pela instituição. Foram três dias de trabalho para questionar os usuários de uma população total de 2040 usuários, o que proporciona uma taxa de erro de oito por cento (8%) e confiança na amostra de noventa por centro (90%).

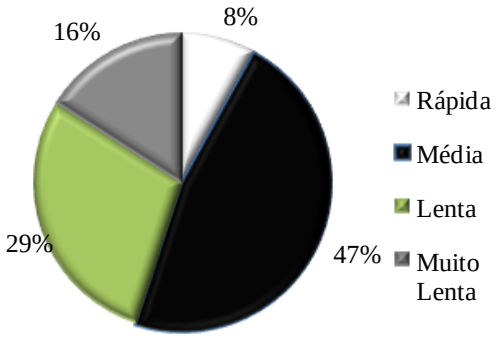
Figura 1 - Grau de satisfação do desempenho da rede



Fonte: Elabroadoa pelo autor

Como pode ser observado nas Figura 1 e Figura 2, os usuários não estão totalmente insatisfeitos com o desempenho do acesso à Internet na instituição. Cinquenta por cento (50%) dos usuários avaliaram como médio o desempenho da rede. Uma pequena parte, apenas doze por cento (12%) dos usuários avaliaram como rápida. O restante, trinta e oito por cento (38%) dos usuários, avaliaram como lenta ou muito lenta.

Figura 2 - Grau de satisfação do desempenho de download

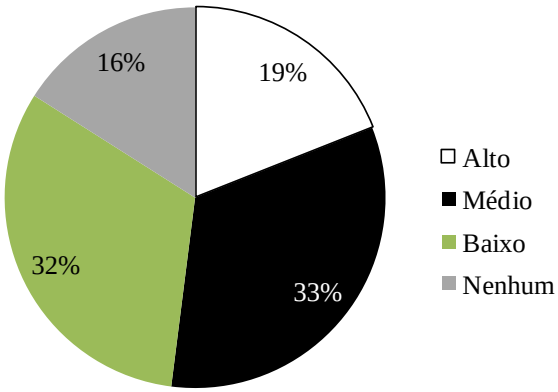


Fonte: Elaborado pelo autor

Também pode ser observado que vários alunos utilizam a rede para baixar arquivos (música, filmes, livros entre outros), evidenciando aí um das causas do congestionamento da rede, enquanto um usuário faz download de determinados arquivos, vários outros tem dificuldade para abrir aulas online, ver e-mails e fazer suas pesquisas.

O grau de conhecimento dos usuários sobre SI, se nunca ouviram falar do assunto ou se sabem da importância, pode ser avaliado na Figura 3. A maior parte avaliou seu conhecimento como médio, trinta e três por cento (33%) e baixo, trinta e dois por cento (32%). Apenas dezenove por cento (19%) dos usuários avaliaram como alto. Os dados, se comparados com a Décima Pesquisa Nacional de Segurança da Informação feita pela Módulo (2006), com 600 usuários de diversas empresas, tiveram resultados bem parecidos.

Figura 3 - Conhecimento do usuário sobre segurança da Informação

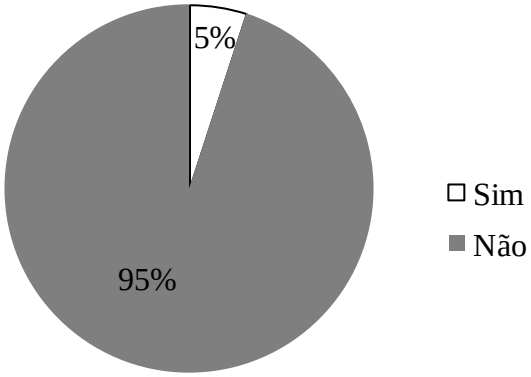


Fonte: Elaborado pelo autor.

Com o objetivo quantificar o número de ocorrências que podem ser classificadas como incidente de SI, conforme a Figura 4, cinco por cento (5%) dos usuários, ou seja, apenas cinco usuários, afirmaram ter sido vítimas de algum tipo de Incidente de Segurança da Informação, uma porcentagem baixa.

Por outro lado, nove por centro dos usuários já tiveram ou já ouviram comentários sobre roubo de dispositivos na instituição, o que também caracteriza um incidente de segurança, pois os conteúdos dos dispositivos ficam indisponíveis e vulneráveis a ataques.

Figura 4 - Incidentes de segurança sofridos



Fonte: Elaborado pelo autor

5.2 Proposta de Política de Segurança

Nesse capítulo será apresentada uma proposta de PSI com o objetivo de aperfeiçoar o nível da Segurança da Informação dentro de uma instituição de ensino superior com ênfase em proteger os recursos da rede, das estações de trabalho e dos equipamentos de informática. Essa Política regulamentará o uso de serviços com o objetivo de diminuir as vulnerabilidades presentes e os incidentes constatados na pesquisa.

5.3 Política de uso da Internet e da rede sem fio

Para regulamentar o acesso à Internet pela rede sem fio da instituição foram estabelecidas normas de uso contidas na PSI, como especificado abaixo:

- Com o intuito de ter maior segurança, o acesso só pode ser feito por equipamentos e usuários autorizados pelo servidor de autenticação aumentando a segurança e diminuindo o número de usuários não autorizados na rede, também não permitindo qualquer tipo de tentativa de acesso não autorizado.
- Com o objetivo de proteger os dados dos usuários, uma norma que não permite a alteração de dados de terceiros, mantendo a autenticidade e a integridade foi implementada. Neste caso, há a necessidade de esclarecimentos e treinamento aos usuários que costumam disponibilizar seus dados pessoais.
- Os usuários que desejarem utilizar os recursos da rede, devem procurar o departamento de TI para que sejam cadastrados, liberando assim seu acesso à rede local. Este procedimento foi adotado pelo departamento de TI. O Proxy da unidade é quem faz o bloqueio dos serviços e qualquer tentativa com a finalidade de buscá-lo como a utilização de Proxys externos não é permitida. Neste caso quando o infrator for identificado responderá administrativamente.
- Outras atividades referentes ao uso da rede dentro da instituição limitadas pela PS ou por regras do Proxy devem ser comunicadas e autorizadas pela equipe de TI. O mesmo procedimento deve ser seguido para os alunos.

5.4 Termo de responsabilidade na utilização dos recursos de rede da instituição

Foi elaborado um termo de responsabilidade focado na utilização dos recursos de rede da instituição, com o objetivo do usuário declarar o conhecimento das normas estabelecidas na política.

5.5 Política de uso das estações de trabalho e dos equipamentos de informática

Com o intuito de regulamentar o uso das estações de trabalho, dos equipamentos de informática da instituição e proteger os seus ativos foi elaborada uma norma informando que não é permitido qualquer tipo de alimento ou bebida nos laboratórios e nas bancadas onde estão as estações de trabalho.

Essa norma também proíbe as mudanças na disposição das máquinas, dos equipamentos de rede, dos cabos de energia e dos cabos de rede, para evitar problemas decorrentes de alterações nas instalações e configurações. Esse problema foi relatado pelo departamento de TI como causador de prejuízos para a instituição.

O usuário, contribuindo com a ordem e a organização das estações de trabalho estará não só cooperando com a equipe de TI, mas também com sua a própria segurança, pois quanto melhor a organização, menor o risco de se danificar os dispositivos.

A norma contida na PSI recomenda aos usuários fazer cópia de segurança de seus arquivos em dispositivos removíveis. O departamento de TI já recebeu vários usuários reclamando terem perdido seus arquivos. A mesma norma recomenda ao usuário fazer "*logoff*" de área de trabalho ao se ausentar, inibindo a ação de indivíduos mal intencionados. Um procedimento tão simples que pode aumentar em muito a SI.

Uma norma proibindo o armazenamento de filmes e jogos nas estações de trabalho foi elaborada. Os recursos de armazenamento são disponibilizados para fins acadêmicos e profissionais, por isso a proibição.

Com finalidade de fazer com que o usuário preste mais atenção em seus pertences foi recomendado que zelem por suas mídias que contem informações pessoais ou da instituição. É muito comum o usuário esquecê-las na estação de trabalho.

Com meta de proteger os equipamentos, foi elaborada uma norma proibindo a saída do laboratório de equipamentos de informática sem a autorização da equipe de TI.

Pelo mau costume da solicitação de serviços ao departamento de TI sem o registro no sistema, muitas vezes feitas informalmente, foi estabelecida uma norma na qual mesmo deve ser feito através de chamados à central de serviços. Todo e qualquer serviço que os colaboradores solicitarem só serão atendidos se constarem na central de serviços, através da abertura de chamados, os quais serão atendidos de acordo com o nível de prioridade e a fila de chamados abertos. Estas informações servirão para uma análise de incidentes futura.

5.6 Termo de responsabilidade na solicitação de notebook e outros equipamentos de informática

A saída de equipamentos sem um termo de responsabilidade é uma falha de segurança, pois caso não ocorra a devolução do mesmo não haverá prova por escrito de quem e quando retirou o mesmo da instituição. Desta forma foi elaborado um termo de responsabilidade para solicitação de notebook e outro equipamento de informática, na qual o usuário terá que

declarar ter lido e concordado com a política de uso das estações de trabalho e dos equipamentos de rede da instituição, assumindo qualquer responsabilidade sobre seus atos e de responder administrativamente caso danifique ou não devolva o equipamento.

6 CONCLUSÕES

O aprimoramento da tecnologia fez com que os usuários se tornassem dependentes dos benefícios concedidos por ela. É um requisito básico e de extrema importância os meios de comunicação de uma instituição, a indisponibilidade desses recursos podem causar impactos promovendo grande prejuízo.

Com o crescente uso da tecnologia, a informação passou a ser um ativo importante e essencial para os negócios, como qualquer outro ativo dentro de uma organização e consequentemente necessita ser adequadamente protegida das ameaças e vulnerabilidades a que estão expostas.

Como pôde ser observado nesta pesquisa, alguns dos principais fatores que colaboram com os problemas de segurança e disponibilidade de recursos da rede é o acesso a sites de filmes, redes sociais e a permissão para "*download*". Esses fatores roubam uma quantia de banda considerável, deixando toda a rede com um tráfego muito lento. A proposta foi a elaboração de uma PSI para ser utilizada nas áreas de trabalho e na rede local, estipulando normas para inibir a utilização dos recursos por pessoas não autorizadas e a sua utilização para outros interesses que não acadêmico, assim como padronizar seu uso, diminuindo o problema da lentidão no tráfego na rede e protegendo os ativos da instituição.

Para a otimização dos serviços prestados pelo departamento de TI, quanto a suporte e manutenção, foram estabelecidas normas para solicitação do mesmo, criando desta forma um banco de dados de incidentes que servirão para os futuros ajustes nas normas estabelecidas.

Uma PSI só produz resultados se devidamente disponibilizada, divulgada e dado o devido treinamento a todos os seus usuários.

Como proposta de continuidade desse trabalho recomenda-se a análise dos resultados a fim de verificar o grau de segurança atingido e manter o processo de melhoria contínua desta política.

7 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS ISO/IEC 27001:2006. **Sistema de gestão de segurança da informação.** Disponível em <http://www.renatodacosta.net/27001.pdf> Acessado em 18 de Outubro de 2011.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR ISO/IEC 27002:2005. **Código de prática para a gestão da segurança da informação.** Disponível em <http://newmoro.blogspot.com/2010/07/nbr-iso-27002-para-download.html> Acessado em 18 de Outubro de 2011.

CAMPOS, Ricardo. **Informação é poder.** Disponível em <http://ricardocampos.wordpress.com/2008/03/03/informacao-e-poder/> Acessado em 29 de Março de 2012.

COURY, Wilson Biancardi. **Poder e Informação**. *Disponível em* <http://www.timaster.com.br/revista/artigos/main_artigo.asp?codigo=424> Acessado em: 17 de Abril de 2012.

DANCHEV, Dancho. **Building and Implementing a Successful information Security Policy**. Disponível em <http://www.windowsecurity.com/pages/security-policy.pdf> Acessado em 20 de Outubro de 2011.

FERREIRA, Fernando N.F. ; ARAÚJO, Márcio T. **Política de Segurança da Informação: Guia Prático para Elaboração e Implementação**. 2 ed. Rio de Janeiro: Editora Ciência Moderna Ltda, 2008.

FINNE, T. A Conceptual framework for information security management. **Computers & Security**, v. 16, n. 6, p. 303-307, 1998.

GABBAY, M. S. Fatores influenciadores na implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação em empresas do Rio Grande do Norte. Tese (mestrado) – Universidade Federal do Rio Grande do Norte

GUIMARÃES, Cesar. **A política externa dos Estados Unidos**: da primazia ao extremismo. Disponível em: < http://www.scielo.br/scielo.php?pid=S0103-40142002000300005&script=sci_arttext> Acessado em 20 de Outubro de 2011.

LYRA, Maurício R. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

MÓDULO. **Décima pesquisa nacional de segurança da informação**. Anuário Estatístico 2006. Disponível em:<http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf> Acessado em 24 de Maio de 2012.

NAKAMURA, Emilio T. ; GEUS, Paulo L. **Segurança de Redes em Ambientes Corporativos**. São Paulo: Berkeley Brasil, 2002.

OLIVEIRA, A. C. **Tecnologia de informação: competitividade e políticas públicas**. Revista de Administração de Empresas, v. 36, n. 2, p. 34-43, 1996.

PIGNATARI, Décio**., Comunicação Informação, Linguagem**. 25. ed. Cotia: Ateliê Editorial, 2002.

STONER, J. A. F. **Administração**. 5. ed. Rio de Janeiro: LTC, 1999.

WARD, J., P. GRIFFITHS e P. WHITMORE, **Strategic Planning for Information Systems**, John Wiley & Sons, Chichester, 1990.

WIENER, Norbert**. Cibernética e Sociedade: O Uso Humano de Sêres Humanos**. Ed 2. São Paulo: Cultrix, 1954.