OS CUIDADOS NA UTILIZAÇÃO DE DISPOSITIVOS TECNOLÓGICOS PARA COMUNICAÇÃO *WI-FI*: UM ESTUDO DE CASO EM EMPRESA ALIMENTÍCIA NO ANO 2010

GUARNIERI, Pamela Yonara
Faculdade Santa Lúcia
pamelaguarnieri@hotmail.com

NETO, Francisco Hyppolito
Faculdade Santa Lúcia
f_hyppolito@hotmail.com

SILVA, Fernando Dionísio da
Faculdade Santa Lúcia
fer.ds@hotmail.com

TROVA, Rosângela Valim
Faculdade Santa Lúcia
prof.msc.rosangela@gmail.com

RESUMO

Este estudo trata da importância do uso seguro dos recursos tecnológicos de comunicação, visto que a informação transformou-se no fator diferencial de competitividade no ramo empresarial, além de facilitar a comunicação nas atividades diárias da sociedade como um todo. O estudo de caso descrito no decorrer do trabalho demonstra as dificuldades de uma empresa em oferecer acesso seguro à rede global da Internet, tanto para si, quanto aos seus clientes, apresentando em seguida formas de promover este acesso com segurança, diminuindo sua vulnerabilidade. Estes e outros aspectos, como os problemas relacionados ao uso correto, principalmente de dispositivos móveis são abordados neste artigo, que considerou

Recebido em 30-08-10 • Aceito em 21-02-11

dados obtidos em pesquisa bibliográfica e de campo. Com o emprego da segurança na disponibilização dos serviços de acesso à rede, observou-se que a empresa adquire vantagem competitiva, além de resguardar suas informações de ações externas.

PALAVRAS-CHAVE: *segurança da informação; dispositivos de comunicação; padronização das atividades.*

INTRODUÇÃO

A tecnologia pode ser a chave de sucesso para o desempenho e crescimento pessoal e profissional, mas ao mesmo tempo faz com que pessoas desobedeçam às leis e tirem benefícios dos outros, principalmente no que diz respeito à privacidade das informações, fazendo desta segurança, o maior desafio para a indústria tecnológica.

Na primeira seção deste trabalho será apresentada uma pequena introdução sobre os temas abordados, em que o ponto chave visa à demonstração dos impactos causados pelo mau uso de recursos e meios de informação.

A segunda seção aborda o uso dos recursos tecnológicos e os perigos de sua utilização em ambientes públicos, focando os problemas diversos para aqueles que não se preocupam com suas próprias informações por meio de sistemas de segurança.

Os sistemas ativos de segurança visam evitar que investidas estruturadas sejam feitas por pessoas mal intencionadas, explorando brechas e vulnerabilidades com objetivos escusos de penetrar no sistema (TORRES, 2001).

Na seção três deste trabalho as informações são voltadas para as redes *wi-fi*, informando os tipos de riscos decorrentes de sua utilização sem requisitos mínimos de segurança além de citar os meios de prevenção para uma utilização segura.

A empresa *Microsoft* (2010), indica que as formas de se obter mais segurança em redes residenciais devem começar com a atenção na escolha certa de senhas de acesso e a forma de armazená-las com segurança, devendo elas ser tratadas com o mesmo cuidado que as informações que protegem.

Na quarta seção, o embasamento teórico está voltado para a utilização de tecnologias móveis e o conhecimento mínimo de segurança e cuidados que seus utilizadores devem ter com seus aparelhos.

Recebido em 30-08-10 • Aceito em 21-02-11

Geddes (2010), cita que os utilizadores de telefones móveis poderão manter registros da saúde, guardar dinheiro e até fazer transações de pequenos valores com seus aparelhos portáteis, e aos criminosos desta nova era da informação não faltarão armas para aplicação de golpes, principalmente para aqueles que não se preocupam com segurança.

Na quinta seção, demonstra-se um estudo de caso em que o uso de recursos tecnológicos de precaução e a aplicação de sistemas ativos de segurança são vitais para a preservação da privacidade e proteção das informações.

As soluções de segurança, desde que sejam corretamente configuradas, são seguras o suficiente para fazer qualquer administrador de rede sentir-se tranquilo no que diz respeito à integridade das informações (TORRES, 2001).

Diante destas abordagens, a última seção apresenta as considerações finais sobre os assuntos tratados, com comentários explicativos dos temas levantados sobre segurança em suas diferentes formas de aplicação.

2. O RISCO DA UTILIZAÇÃO DOS MEIOS DE COMUNICAÇÃO EXISTENTES

Tanenbaum (2003) revela que embora a indústria da informática seja jovem, torna-se cada dia mais possível oferecer vantagens no cotidiano das pessoas, em seu ambiente de trabalho. Antigamente eram poucas as pessoas que dispunham de recursos financeiros e tecnológicos para a utilização de computadores nas atividades diárias.

Estão disponíveis inúmeros recursos de comunicação que possibilitam rápidos e eficientes contatos entre as pessoas com as quais desejamos nos relacionar, sendo possível também a realização de eventos e agendamentos diários (TANENBAUM, 2003).

Segundo Torres (2001), deve-se fazer o uso de ações que evitem a danificação e comprometimento dos dados, no intuito de impossibilitar a origem de um problema ou consequências desastrosas causadas por pessoas mal intencionadas. Dentro dessas ações estão os antivírus e *softwares* específicos que monitoram e rastreiam o funcionamento do sistema a fim de proteger e restringir uma ação ou comando que esteja fora da política de segurança.

Independente do ambiente de onde as informações são geradas torna-se necessário que se estabeleça o mínimo de segurança possível, evitando situações de riscos que possam ser prejudiciais tanto ao sistema

Recebido em 30-08-10 • Aceito em 21-02-11

quanto para as próprias pessoas que fazem uso de recursos tecnológicos de comunicação (TORRES, 2001).

Para Tanenbaum (2003), os recursos tecnológicos se encontram em inúmeros ambientes, no entanto sua utilização tornou-se tão comum que muitas vezes passam despercebidos. Dentro desse contexto, o conforto adquirido por esses meios pode resultar em transtornos, se não estabelecidos com segurança.

Para Torres (2001), evolução tecnológica proporciona praticidade na execução de grande parte das atividades profissionais e até mesmo pessoais. Porém, inerente a essa situação de conforto destacam-se transtornos que, na maioria das vezes, podem ser evitados com o uso desse avanço para o bloqueio de tal situação.

A necessidade de se estabelecer comunicação de modo ágil é evidente, no entanto torna-se primordial a necessidade no cuidado com situações que possam gerar desconforto, por isso, a manipulação de dados pessoais por meio de recursos tecnológicos sugere o uso de critérios de segurança (TANENBAUM, 2003).

3. O PERIGO DAS REDES *WI-FI*

Existem diversos perigos na utilização de redes de computadores sem fio residenciais que ocorrem, muitas vezes, pelo desconhecimento por parte dos utilizadores que não se preocupam com a proteção ao acesso de seus equipamentos (TORRES, 2001).

Não existe hoje uma rede profissional que não implemente mecanismos de segurança, visando evitar incidentes que causem prejuízos (TORRES, 2001).

Este conceito pode ser transferido para as redes residenciais se pensarmos que, atualmente, muitas atividades cotidianas são realizadas pelas pessoas sem sair de casa por meio do uso do computador e da rede global da *Internet*. Pagamento de contas, compra de produtos, realização de transações entre bancos, todas essas tarefas podem, ao invés de facilitar a vida, criar um grande desconforto se não houver a preocupação com a segurança, e os prejuízos podem vir de diversas formas, causados ou não por agentes externos, os famosos *hackers* (TORRES, 2001).

Outro problema que pode ser ainda mais perigoso do que estar desprotegido, é pensar que está protegido, ou seja, quando temos a falsa sensação de segurança. Isso ocorre principalmente quando utilizamos recursos obsoletos de segurança (TORRES, 2001).

Recebido em 30-08-10 • Aceito em 21-02-11

Percebe-se que de nada adiantam os métodos para impedir que um *hacker* entre em seu sistema se não implementarmos na rede processos de prevenção e controle que diminuam a vulnerabilidade ambiental e resguardem as informações (TORRES, 2001).

Segundo Kleinrock (2009), (apelidado de pai da *Internet*, pois publicou o primeiro trabalho sobre comutação de pacotes[1] em 1961, e coordenou a montagem dos primeiros nós de comutação de pacotes da *Arpanet* em 1969, que mais tarde se transformaria na *Internet*), não existe segurança nos fundamentos da *Internet*, pois durante sua criação, a quantidade de usuários era muito pequena, todos se conheciam e havia muita confiança entre os utilizadores. O autor afirma ainda que a *Internet* é um canal aberto e um dispositivo igualador, em que não importa quem ou o que você faz, na *Internet* todos podem postar uma opinião sem qualquer tipo de permissão.

De acordo com Kleinrock (2009), é esta liberdade que torna a segurança da *Internet* quase impossível, pois além dos perigos externos que possam atingir uma rede privada, ainda temos os perigos internos, em que um colaborador de uma empresa perde muito tempo com informações alheias ao seu trabalho, tornando este um dos lados negros da *Internet*.

3.1. CONHECENDO E PROTEGENDO

Com exceção da segurança física do computador, quase toda segurança se baseia em princípios criptográficos (TANENBAUM, 2003). Essa criptografia nada mais é do que a transformação da informação de sua forma normal para uma forma ilegível de maneira que apenas o seu destinatário possuidor da chave de acesso correta consiga entender.

Para redes residenciais, a maioria dos equipamentos convencionais de transmissão de dados sem fio utiliza os padrões WEP (*Wired Equivalent Privacy***)**, WAP (*Wireless Application Protocol***)** ou WAP2 de criptografia de chaves de acesso para segurança, sendo que o último oferece serviços de segurança, privacidade, autenticação e controle de integridade melhor que os demais (TORRES, 2001).

Para Torres, (2001), outra ameaça às informações vem dos meios físicos que são conectados diretamente nos computadores como *pen-drives*, mídias ópticas ou mesmo os antigos disquetes. Estes itens quando não

[1] Técnica de transmissão que consiste em dividir a informação em pequenos blocos.

Recebido em 30-08-10 • Aceito em 21-02-11

utilizados de forma segura podem trazer consigo vírus que nada mais são do que códigos móveis que entram nos programas do computador causando danos diversos.

Todos os dias são criados novos vírus dificultando até mesmo para as empresas de desenvolvimento de antivírus uma solução ideal. Porém estes *softwares* são indispensáveis, principalmente quando as informações contidas no computador não possuem redundância (*MICROSOFT,* 2010).

A *Microsoft* (2010) aponta alguns passos para proteção de um computador pessoal para redes residenciais, como manter o *Firewall* sempre ativo e atualizar, sempre que solicitado, o sistema operacional, o antivírus e o *anti-spyware*. Estas ações devem ser tomadas principalmente quando estará disponível o acesso à *Internet,* que além de introduzir tecnologia, introduz desafios à proteção da privacidade individual, pois as informações transmitidas passam por diversas redes de computadores antes de chegar ao destino final com a possibilidade de serem monitoradas, rastreadas, capturadas, armazenadas, copiadas e alteradas.

Marciano e Marques (2006) concluem em seu artigo que não se conhece qualquer solução meramente tecnológica para problemas sociais, e sendo a segurança da informação um conceito eminentemente social, necessita de uma visão embasada em conceitos sociais, além dos tecnológicos para sua correta cobertura.

A solução para que os problemas de segurança sejam solucionados depende, além de fatores tecnológicos, de uma mudança na cultura das pessoas que deve ser adequada a esta nova realidade ante o fenômeno da sociedade da informação (MARCIANO; MARQUES 2006).

4. UTILIZANDO A TECNOLOGIA MÓVEL COM SEGURANÇA

Segundo Marciano e Marques (2006), o universo de conteúdo digital está em constante desenvolvimento em relação à comodidade de seus usuários. Diante disso, acaba estando sujeito a diferentes tipos de ameaças, podendo ser físicas ou virtuais, o que comprometeria a segurança das pessoas e das informações a elas referentes.

Marciano e Marques (2006) ainda afirmam que o uso de aparelhos eletrônicos está mais amplo, proporcionando aos usuários diferentes produtos eletrônicos para realizar diversas tarefas que manualmente e pessoalmente demorariam muito tempo. Um exemplo disso, seria acessar o banco através do *notebook*, ou utilizar o GPS (*Global Positioning System*) contido no celular.

Segundo Longo (2003), os aparelhos eletrônicos se tornaram cada

Recebido em 30-08-10 • Aceito em 21-02-11

vez mais essenciais na vida das pessoas. Dessa forma, as preocupações com as informações nele contidas se tornou algo primordial. Dessa maneira, até mesmo as pessoas físicas necessitam de conhecimentos básicos sobre segurança da informação.

Conforme Geddes (2010), existem diversos aparelhos eletrônicos presentes no mercado, como *notebooks, pen-drives*, HD externo e *I-Pod*. Diante disso, percebe-se que um simples celular pode revelar quase tudo sobre a vida do proprietário, podendo conter informações sobre a empresa de trabalho, a rota que a pessoa utiliza todo dia, e até mesmo mensagens e fotos apagadas do *chip,* que ainda continuam na memória do celular.

Geddes (2010) ainda destaca que, embora muitos aparelhos celulares atuais possuam recursos de segurança para as informações, é possível perceber que muitos dos usuários não se utilizam dos mesmos, ficando cada vez mais vulneráveis. Entende-se que para garantir segurança das informações é necessário utilizar-se de todos os recursos disponíveis no aparelho, além de excluir elementos comprometedores logo que chegam à caixa de entrada, mesmo que às vezes estes possam ainda estar na memória do celular.

De acordo com Marciano (2006), a multiplicação do uso de sistemas de informação para atividades que envolvem suas bases de dados integrados com a rede, pode ser um dos fatos determinantes na sociedade da informação.

Finalizando, Araújo (1991) cita que o principal desafio em relação à tecnologia e segurança das informações seria primeiramente o aprimoramento do próprio ser humano, como um pré-requisito para que a tecnologia e o conhecimento técnico consigam continuar a se desenvolver sem ameaçar a qualidade de vida do homem e, principalmente, a segurança da humanidade.

5. METODOLOGIA

O presente trabalho apresenta um estudo de caso que tem o objetivo de ilustrar a importância da aplicabilidade da segurança da informação, relatando os problemas enfrentados por uma empresa para promover utilização de tecnologia sem fio de acesso à rede global da *Internet,* de forma confiável e segura.

A empresa em estudo trabalha no ramo alimentício e foi fundada em 1985, no município de Mogi Mirim, localizado no estado de São Paulo. Nessa ocasião, contava inicialmente com sete funcionários para atendimento, e hoje a empresa, além de possuir uma nova filial na cidade de Rio Claro,

Recebido em 30-08-10 • Aceito em 21-02-11

ainda conta com um quadro de cento e trinta funcionários divididos entre as duas unidades.

Percebe-se que com a alta competitividade de mercado, a utilização de mecanismos para busca de novos clientes oferecendo, além de qualidade dos produtos comercializados, formas de entretenimento que atraiam diferentes públicos, tornou-se um fator diferencial para as empresas de qualquer ramo de atividade. Além disso, com a invasão dos dispositivos móveis de comunicação que possuem recursos de conexão com a *Internet*, as empresas passaram a utilizar o acesso de rede sem fio como um dos meios de obter vantagem competitiva.

A empresa em estudo, quando realizou-se esta pesquisa, fornecia a seus clientes, conexão livre de acesso a *Internet*. Porém, por meio de um estudo direcionado à segurança desse serviço oferecido, foi possível detectar diversos problemas que estão causando incômodo tanto para clientes quanto para a própria empresa. O levantamento desses problemas, bem como as possíveis soluções para sua correção, serão detalhados nos tópicos seguintes.

5.1. LEVANTAMENTO DO PROBLEMA

Para levantamento do problema, foi inicialmente desenvolvido um questionário com 15 questões abertas, estruturadas e não disfarçadas, direcionadas aos donos da empresa, com questionamentos diversos para conhecer a forma como o serviço de *Internet* é disponibilizado para os clientes e funcionários. Nesse questionário as perguntas estavam relacionadas não só com o nível de segurança que a empresa possui para promover o acesso a seus clientes, mas também com o nível de conhecimento de seus colaboradores para o uso da tecnologia disponível. Além disso, a entrevista propõe também questões sobre o nível de conhecimento dos proprietários sobre esses serviços e a segurança da rede sem fio, fatores que são de suma importância para determinar a forma com que a solução deve ser implementada.

Dentre as diversas questões feitas aos donos da empresa, pôde-se verificar que a empresa possui um roteador configurado para permitir acesso somente com uso de senha, que é trocada a cada dois meses, fazendo uso do padrão de tecnologia WEP. Esta rede, disponibilizada a no máximo oito clientes, não está interligada à rede da empresa.

A empresa divulgou que possui contrato com um técnico de informática que faz o suporte em seus equipamentos quando há algum problema. Além disso, os colaboradores são instruídos a utilizar os computadores

Recebido em 30-08-10 • Aceito em 21-02-11

somente para fins relacionados às suas atividades, mas não existe um controle sobre essas ações.

Quando questionada sobre o nível de conhecimento de seus colaboradores para informações aos clientes sobre acesso, ou mesmo, cuidados que os clientes devem ter na utilização da rede, os entrevistados disseram que não saberiam instruir os clientes sobre a forma tecnicamente indicada de acesso.

Por fim, a empresa afirma estar enfrentando problemas na disponibilização desse recurso, já que muitas vezes os clientes não conseguem acessar a rede e não possuem conhecimento para identificar o problema.

Com base nesse questionário, observou-se que a empresa já conta com o atendimento de um profissional da área de tecnologia da informação e também possui um serviço de criptografia para acesso de sua rede sem fio e um esquema de alteração de senhas. Porém, observou-se que os recursos utilizados estão com padrões técnicos obsoletos.

A forma de gerenciamento desses meios de comunicação também está sendo realizada de modo a favorecer possíveis tentativas de invasão e ações de usuários maliciosos.

Faz-se necessário destacar que o proprietário da empresa em estudo não autorizou a divulgação do exemplo de invasão que a empresa enfrenta.

Observou-se que o desempenho da rede é prejudicado pela localização do roteador, que se encontra entre diversos obstáculos sendo eles, o forno utilizado na manufatura dos produtos da empresa, as portas de vidro e o aquário.

As **Figuras 1** e **2** apresentam a localização do roteador quando da realização do levantamento do problema, bem como, os obstáculos que podem estar causando os ruídos no sinal, prejudicando assim, o acesso à rede sem fio da empresa.

Figura 1 – Roteador

Recebido em 30-08-10 • Aceito em 21-02-11

Figura 2 - Localização do roteador

Quanto ao padrão de criptografia utilizado pela empresa atualmente (WEP), já foi demonstrado na seção 3 que este tipo de criptografia não oferece uma forma de segurança que contemple exatamente os quesitos básicos desejáveis para uma proteção adequada quanto à segurança, privacidade, autenticação e controle de integridade das informações.

A modificação de senha a cada dois meses também possibilita que o uso desse recurso de rede, que deveria beneficiar apenas os clientes que estão consumindo no momento, seja utilizado de maneira descontrolada, visto que, o perímetro de alcance da rede ultrapassa os limites físicos da empresa. Esse processo permite a qualquer pessoa fora desse ambiente, de posse da senha, consiga acessar a rede.

O problema analisado já ocorreu na empresa, visto que a utilização da rede sem fio estava sendo feita pelas residências vizinhas sem autorização da empresa, ocorrência relatada pelo proprietário da empresa.

Devido à falta de gerenciamento da rede e durante as ocorrências dos problemas relatados pelos clientes na tentativa de acesso à rede sem fio, os administradores do negócio acabam atribuindo falsos diagnósticos para estes inconvenientes. Um exemplo claro é a ausência de informações por parte dos funcionários, no momento de orientar os usuários sobre a melhor forma de utilizar a rede. Além disso, sem o controle dos acessos, fica impossível saber se o problema está na supressão de usuários conectados,

Recebido em 30-08-10 • Aceito em 21-02-11

nos obstáculos que diminuem o sinal do roteador, ou mesmo se está sendo causado por acessos indevidos.

5.2. SOLUÇÃO

Quando uma empresa enfrenta problemas que não estão diretamente relacionados com as atividades do seu principal negócio, e até mesmo por ser um problema que aparentemente não traz prejuízo significativo na contabilidade final, os administradores acabam não proporcionando a devida atenção para a solução e não percebem os perigos que essas adversidades podem causar em longo prazo.

As informações de uma empresa são parte de seu patrimônio, pois contêm toda sua trajetória, e informações sigilosas de seus valores particulares e de seus funcionários. Sendo assim, a proteção desses dados deve ser motivo de preocupação para seus administradores. Além disso, quando a empresa se propõe a fornecer qualquer tipo de serviço e não atende a demanda, mesmo que esse serviço não seja parte fundamental de sua atividade, acaba refletindo negativamente para os clientes mais exigentes. A insatisfação implica má reputação e, com o tempo, a perda de espaço no mercado para um concorrente mais competente se torna inevitável.

Após as verificações dos problemas que estão ocorrendo na empresa, percebe-se a necessidade da troca do equipamento de distribuição de rede atual por um que suporte maior quantidade de usuários, para evitar que o acesso solicitado não possa ser atendido, conforme cita Tanenbaum (2003).

Ainda por Tanenbaum (2003), o padrão de criptografia utilizado pela empresa deve ser alterado para um que forneça maior segurança e confiabilidade contra ataques externos, como é o caso do padrão WAP2.

Verificando o *layout* da empresa, observou-se que a localização tecnicamente indicada de instalação do equipamento de distribuição de rede, conforme orienta Tanenbaum (2003), deve ser no ambiente externo da empresa, pois os obstáculos não estariam entre equipamento e usuário.

Longo (2003), afirma que quanto à modificação da senha de acesso, a periodicidade de troca deve ser feita diariamente, evitando assim o perigo de se ter usuários indevidos, assim como o tipo de senha utilizado não pode obedecer a um padrão de fácil entendimento como, por exemplo, a utilização da data atual, de maneira que os usuários por si só consigam adivinhar a senha.

A **Figura 3** apresenta o novo local de instalação do roteador na empresa, escolhido de forma a proporcionar a melhora do sinal e a diminuição de problemas ocasionados por obstáculos, e de acordo com ensinamentos de Longo (2003).

Recebido em 30-08-10 • Aceito em 21-02-11

Figura 3 - Nova localização do roteador

Após todas as mudanças relatadas será necessária a realização de um treinamento com os funcionários que terão contato efetivo com esse recurso de rede, para que eles tenham capacidade de monitorar e controlar o acesso dos clientes à rede de acesso sem fio da empresa.

É importante salientar que todas as medidas de segurança citadas não irão garantir, integralmente a segurança das informações da empresa se não houver também uma mudança na atitude dos envolvidos para manter as ações em constante uso, devendo, a partir deste momento, tornar a segurança do serviço de rede, parte das atividades diárias da empresa.

CONSIDERAÇÕES FINAIS

Nota-se que a evolução das tecnologias de comunicação, como *Wi-Fi*, possibilitou uma grande comodidade para seus usuários, ao passo que sua conexão permite o fluxo rápido de dados entre as diferentes redes remotas. Porém, torna-se necessário utilizar tais recursos com cautela, pois, apesar de apresentarem inúmeras comodidades, a segurança da rede *Wi-Fi*, pode ser facilmente burlada caso não se estabeleçam parâmetros para proteger os dados de seus usuários específicos.

Dentre os perigos existentes na manipulação de dados pessoais, pode-se destacar o uso de redes de computadores sem fio, que por se tratar de um meio de conexão e acesso rápido, tem maior incidência de tentativas de invasões. No entanto existem meios de proteção como o padrão WAP2

Recebido em 30-08-10 • Aceito em 21-02-11

de criptografia de chaves de acesso para segurança, entre outros, que visam proporcionar um ambiente mais seguro e confiável a seus usuários.

Outro aspecto muito importante é o fato de que estes recursos visam facilitar a forma de relacionamento e comunicação entre seus usuários, assim como auxiliar no cumprimento de seus compromissos e acesso à *internet* ou até mesmo em movimentações bancárias. Criou-se uma grande dependência desse universo de conteúdo digital, que tem evidenciado seus diferentes tipos de ameaça, que podem ser fiscais ou virtuais.

Para demonstrar a utilização de segurança da informação, foi realizada a elaboração de um estudo de caso observando os problemas enfrentados em uma empresa, juntamente com a apresentação de uma solução para eles. Essa metodologia possibilitou a representação e a exposição das necessidades e mecanismos utilizados para satisfazer e alcançar os objetivos do cliente, evidenciando que para isso, não é preciso deixar de contemplar também os fatores de segurança necessários a qualquer meio de transmissão e captação de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO, V. M. R. H. de. **Informação:** instrumento de dominação e submissão. Brasília Janeiro/Junho, 1991 Disponível em: <http://revista.ibict.br/ciinf/index.php/ciinf/article/view/1226/866> Acesso em março de 2010.

GEDDES, L.. Sua vida num celular roubado**. Revista Info Exame**. nº 287 Publicação mensal. São Paulo: Abril, Janeiro de 2010.

KLEINROCK, L.. O preço da Liberdade. **Revista Informática Hoje**. nº 625 Publicação mensal. São Paulo: Plano Editorial, Setembro de 2009.

LONGO, G. D.. **Segurança da informação**. São Paulo Dezembro, 2003. Disponível em: <http://www.firewalls.com.br/files/ArtigoCientifico.pdf> Acesso em março de 2010.

MARCIANO, J. L. P.. **Segurança da Informação –** uma abordagem social. Brasília Setembro, 2006 Disponível em: <http://docs.docstoc.com/orig/970374/0b549151-a638-4d40-b962-5ddae2429eac.pdf> Acesso em março de 2010.

MARCIANO, J. L.; MARQUES, M. L.. **O Enfoque Social da Segurança da Informação**. Brasília Setembro/Dezembro, 2006 Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652006000300009&lang=pt> Acesso em março de 2010.

Recebido em 30-08-10 • Aceito em 21-02-11

MICROSOFT. **Quatro Passos para Proteger seu Computador.** Disponível em <http://www.microsoft.com/brasil/protect/computer/default.mspx> Acesso em março de 2010.

TANENBAUM, A. S.. **Redes de Computadores**. 10ª Edição - Rio de Janeiro: Campus, 2003.

TORRES, G.. **Redes de Computadores** – Curso Completo. Rio de Janeiro: Axcel Books, 2001.

Recebido em 30-08-10 • Aceito em 21-02-11